SYNOPSIS OF PhD DISSERTATION

E-commerce security and its regulation: Vulnerable individuals in e-commerce

by

Narmin Miriyeva

Co-supervisors:
Professor Dr. Mezei Péter, Ph.D.
Associate Professor Dr. Csatlós Erzsébet, Ph.D.

Doctoral School of Law and Political SciencesUniversity of Szeged
Szeged, 2024.

Table of Contents

I) Background of the research 3

1. The aim of the research 8

2. The research questions 8

3. The research objectives 9

4. The methodology of the research 10

5. Contribution to scientific field 12

6. The structure of the research work 13

II) Scientific results and recommendations 15

III) The list of the author's publications written within the topic of the dissertation 21

I) Background of the research

Society is on the cusp of the digital world, which has been triggered by the explosion in information technology and, therefore, the rapid growth of the Internet. The phenomenal growth of the Internet and the World Wide Web has also influenced adjustment in the daily lives of users and the fate of entrepreneurs in online markets. The Internet have intensified the spread of the electronic revolution, and because of the collaboration, a new network revolution has entered the scene.

The conjunction of Internet networks, website designs, and computer devices created a new wave of trade: electronic commerce or e-commerce. This is expressed in any form of business transaction where the parties communicate electronically, rather than via physical exchanges. Electronic commercial transactions are one of the key components of e-commerce that are carried out outside of national borders by private individuals and commercial entities. The concept of e-commerce transactions consists mainly of three components: electronic means, commerce, and transactions. Electronic means are the way and route of sale and purchase. Commerce is the basic essence of the operations and their substance. The transaction is the goal and result of the operation or activities.[1]

Improvements in the information technology and continuous entrepreneurial innovation in business and marketing assure that there will be as many changes in the next ten years as they have in the last two decades. The 21st century will be the century of digitally activated social and commercial life, the outlines of which can be barely seen now. Assumably, e-commerce will ultimately affect almost all forms of commerce, and most of the trade by 2050, if not sooner, will be e-commerce.[2]

E-commerce is an appealing area for anyone who wants to generate new ideas or who would like to innovatively bring them to life. Major technological advances in computers and communications continue at a rapid pace. E-commerce appeals equally to people with a passion for fundamental problems and a desire to make transformative contributions.[3]

Many researchers and executives recognise the rise of e-commerce not only as a distinct field of industry but also as the most important economic development of the

[1] Faye Fangfei Wang, *Internet Jurisdiction and choice of law: Legal practices in the EU, US and China*, Cambridge University Press, Cambridge, 2010, 1.
[2] Kenneth C. Laudon & Carol Guercio Traver, *E-commerce: business, technology, society*, Boston, Pearson, 2017, 8.
[3] Steven O. Kimbrough & D.J. Wu (eds), *Formal Modelling in Electronic Commerce*, Berlin, Springer, 2005, 1.

period. The world is undergoing tremendous changes in a way business is done due to the rapid implementation of technologies by businesses. The new business environment created by e-commerce is not an imaginary vision of technocrats, but rather a new 'global order' in which millions of dollars are exchanged between parties every day. In formulating corporate strategy and developing value, the role of e-commerce is undeniable. In addition, e-commerce also transforms our society and culture as we know it.[4]

The retail world is on an unprecedented wave of innovation. Technology plays a significant role, of course, but it's not the only force at work. New business models are evolving that will have a profound impact on e-commerce and the wider retail value chain. At the same time, the attitudes and preferences of consumers are changing. Today's e-commerce consumer is largely directed by price and convenience: doing business with products that ship quickly. These basic preferences will still exist by 2026, but along with the shopping experience, consumer perceptions of the e-commerce experience will have changed dramatically.[5]

With the acceleration of digital transformation, the e-commerce landscape is becoming more dynamic. Along with taking on new roles of existing actors, new actors emerged. Some business, individual and country barriers to e-commerce have been overcome, but new ones have emerged. New opportunities have emerged to unlock the potential of e-commerce and increase consumer growth and wealth. E-commerce was primarily designed to enable repeat transactions between large companies and relied on configurable networks for electronic data interchange. E-commerce is now expanding to smaller businesses with the expansion of open networks such as the Internet and is increasingly used for transactions between firms and customers. Although the e-commerce landscape is still dominated in absolute terms by transactions between businesses, the adoption rate is currently, on average, faster in industries where consumers play a significant role, such as retail or accommodation.. These dynamics are supported by universal access to the Internet via mobile devices, as well as modern payment methods.[6]

---

[4] Celia T. Romm & Fay Sudweeks (eds), *Doing Business Electronically: a global perspective of electronic commerce*, London, Springer-Verlag Limited, 2000, 1.
[5] Ovum Report, 'The Future of E-commerce: The Road to 2026,' 2017, 12.
[6] OECD, 'Unpacking E-Commerce: Business Models, Trends and Policies', Paris, OECD Publishing, 2019, 32.

E-commerce is based on Internet technology. Overall, internet technology and information technology are the protagonists of the game. Without the Internet, e-commerce would hardly exist. However, e-commerce is not only about business and technology. The third part of the equation for understanding e-commerce is society. E-commerce has important social implications that managers can only ignore at their own risk. E-commerce has questioned the concepts of privacy, intellectual property, and even national sovereignty and governance. Managers need to understand these social improvements by accepting that the Internet is limitless, transcends social governance and regulation, or Internet is a place where market efficiency is the only factor.[7]

However, concerns about the physical store's demise are overblown, as e-commerce is expected to account for only 21% of overall retail sales and 5% of food sales by 2023. To begin with, consumers prefer to purchase from the comfort of their own homes rather than going to the nearby shopping mall. Moreover, brick-and-mortar retailers are dealing with an increase in the complexity of stock-keeping units; in a world of ever-shorter product cycles and rapid innovation, stock-keeping units have expanded quickly. Additionally, the highly digitised and knowledgeable online consumers of today have higher standards for customer service and experience, which calls for both more time spent with customers and frontline staff with better training.. Additionally, the rise of omnichannel experiences is altering the core purpose of physical stores. Stores are projected to provide a growing number of omnichannel services, such as in-store fulfilment and online purchase returns.[8]

The COVID-19 has further emphasised the move to e-commerce as people and businesses have gone online to deal with several lockdown actions and travel restrictions. The crisis has also highlighted the significant digital divide between and within countries that characterise the world and raised fears that digital transformation will lead to increasing digital divides and inequalities. In different trade deals, governments are giving growing attention to the treatment of e-commerce. Given that countries are at very different stages of e-commerce readiness and offer different priorities for different trade policy objectives, their reactions to the changing environment vary considerably.[9]

---

[7] Laudon & Traver, *E-commerce,* ix.

[8] McKinsey & Company, 'Future of retail operations: Winning in a digital era', Issue 2, McKinsey & Company, 2020, 4-9.

[9] UNCTAD, 'What Is at Stake for Developing Countries in Trade Negotiations on E-Commerce? The Case of the Joint Statement initiative' UNCTAD Research Paper, 2021, v.

Although consumer protection has constantly been concentrated on defending the weaker party - the consumer, modern data-driven services, regardless powerful and advantageous they may be, frequently seem to put the consumer in a worse position than before. Traders profit from behavioural findings provided by datasets that frequently compile information from users' full history of Internet interactions, including search histories, email, and instant message histories, browsing patterns, or forecasts of financial state. Consumers must deal with ever-evolving option infrastructures that are constantly being updated to optimise engagement and conversion rates.[10]

Since consumers are typically the weaker side in the transactions, it is believed that they should have their health, safety, and economic interests protected. In their interactions with professional traders, all consumers are protected by consumer policy instruments. Nonetheless, certain consumer groups may be particularly vulnerable in certain circumstances and require additional protections. Consumer vulnerability may be influenced by societal factors or specific traits of certain customers or groups of consumers, including age, gender, health, digital literacy, numeracy, or financial condition. The pandemic may have made some forms of vulnerability worse than they were before.[11]

People are increasingly giving personal information to service providers and online platforms, sometimes unintentionally, as internet services and social media become more widely available. In addition to assaults and fraudulent usage occurring often, the digitalisation of information and improved network connectivity provides additional difficulties for the protection of personal data.[12]

The misuse of their personal information to commit fraud is a concern for half of all European Internet users. About seven out of ten consumers worry that their information will be utilised for anything other than what it was intended for. 71% of Europeans believe that if they want to buy goods or services, their only option is to give their personal information. Almost all users from the EU believe that if their data is lost or stolen, they would like to be informed about it. Only 15% of respondents believe they have total control over the data they share online, while 31% believe they have no control over it at

[10] BEUC: The European Consumer Organisation, 'Towards European Digital fairness: BEUC framing response paper for the REFIT consultation', Brussels, 20/02/2023, 4.
[11] European Commission, 'Communication from The Commission to The European Parliament and The Council New Consumer Agenda Strengthening consumer resilience for sustainable recovery', Brussels, 13.11.2020 COM (2020), 696 final, 16.
[12] OECD, 'Measuring the Digital Transformation: A Roadmap for the Future', Paris, OECD Publishing, 2019, 575.

all. Individuals must maintain effective control over personal data in this rapidly changing environment. Every person in the EU has this fundamental right, and it needs to be protected.[13]

The choice of EU law as the study's foundation seems suitable for two key reasons. First of all, even though the EU is a union of sovereign states, each of which has its national laws, all MS must abide by the EU's rules, which reflect the EU's consensus on appropriate legal standards. The doctrine of the direct effect of EU legislation supports this strategy. The CJEU has ruled through this doctrine that EU laws, including the GDPR, are directly applicable and should be construed consistently throughout the Union, with a few exceptions. Moreover, even though the legal, economic, and cultural fragmentation of the EU market is undeniable, there is a common perception and political trend that it is a single market. The concept of a single digital market has gained prominence in recent years on the political agenda of the EU. It is thought that more uniform legal regulations in the digital sphere will lower the administrative costs for EU enterprises and increase citizen protection.[14]

It would not be an exaggeration to state that current e-commerce transactions are an integral part of the lifestyle of online users, given the increasing use of technologies by the population. In this regard, e-commerce corporations can be sure that online consumers' requests will increase over time and will find some solutions through more advanced technologies such as distributed ledger technology and AI. Since online users are the main concern of the EU's DSM Strategy, their security and protection are also connected to e-commerce-related areas in general. The same online user may be identified as both a consumer and a data subject because e-commerce is a multidisciplinary field that can overlap with several legal disciplines. In fact, some online users may be more receptive and vulnerable given that not all users are equally qualified and able to participate in these online relationships. As a result, the concept of vulnerability will be investigated in this work in terms of the protection and safety of vulnerable online users in both the consumer and data protection law disciplines. Finally, the most recent legislative transformations, in the digital industries, notably those relating to e-commerce, will be conducted.

[13] European Commission, Directorate-General for Justice and Consumers, 'How does the data protection reform strengthen citizens' rights?' Publications Office, Factsheet, 2018, 1.
[14] Helena U. Vrabec, *Data Subject Rights under the GDPR With a Commentary through the Lens of the Data-driven Economy*, UK, Oxford University Press, 2021, 12.

1. The aim of the research

The aim of this dissertation is to examine and define the concept of vulnerability and the position of vulnerable individuals in both legal disciplines of consumer protection and data protection. Comparing and analysing the disciplines of consumer and data protection law in relation to the protection and security of the concept of vulnerability for digital sectors could help to mitigate the risks associated with this concept in the future. Since online users take part in e-commerce transactions, the general field of e-commerce as well as its primary subcategories, particularly B2C will be reviewed considering recent EU consumer protection-related cases.

There will be attempts to define this concept and particularly the vulnerable consumer position in online interactions from the consumer protection law field because the concept of vulnerability is not fully recognized in academia. Several current CJEU decisions and prospective current consumer regulatory measures will be taken into consideration with the aim of depicting and defining the position of online vulnerable consumers.

Later, this concept in the field of data protection law will be reviewed with the aim of finding and determining the position of vulnerable online data subjects in the data processing. Regarding the digital transformation, the EU's capacity to implement and provide the regulatory frameworks for the Digital Single Market will be closely examined.

2. The research questions

The research question is regarded as an important initial move that serves as a compass for an investigation. It assists the researcher in linking his or her literature review to the types of data that will be collected. As a result, many accounts of the research method include the formulation of a research question as a stage that aids in the prevention of haphazard data collection and review.[15]

One of the main reasons for addressing these research questions is the start of research on e-commerce as a separate area of law. As a result, the second chapter, which is more informative, begins with e-commerce as a multidisciplinary area of law, but it attempts to provide a starting place and niche for additional academic effort. Individuals

[15] Alan Bryman, 'The Research Question in Social Research: What is its Role?' *International Journal of Social Research Methodology*, vol/10:1, 2007, 5-20.

are one of the key participants in e-commerce transactions, thus their safety and security are, have been, and will always be a priority for the EU. Since not all people are the same and as a result they can be differentiated by mental or physical weakness, age, gender, gullibility, and other factors. These distinguishing criteria demonstrate that while not all individuals may be recognised as the average or standard, some group of individuals may be left outside the circle. Individuals with these distinctive characteristics may feel more susceptible and vulnerable when interacting with others online. Since there is no clear formulation of the concept of vulnerability in general, there is a need to find it and revise existing ones in the scientific community.

Within the research process the following questions will be addressed for further solutions:

a) To what extent can EU define the concept of vulnerability and the position of the vulnerable individuals in the consumer protection law.

b) To what extent can EU explain the concept of vulnerability and the position of the vulnerable individuals in the data protection law.

c) To what extent can EU e-commerce deal with recent regulatory issues?

As can be seen from the research questions the solution will be proposed from the online individuals' perspective, as they are one of the active and susceptible participants in both consumer and data protection legal disciplines. However, the focus will not be on the typical average user group, but on a vulnerable group of individuals who are more likely to be more needy and unaware of ways to be identified and anticipated as 'the vulnerable' to obtain the necessary protection during online transactions.

3. The research objectives

Since there is no clear position on the concept of vulnerability and the vulnerable individuals both in consumer and data protection law disciplines, the following research objectives will be reviewed:

a) to define the position of the concept of vulnerability and vulnerable individuals in the consumer protection law.
b) to determine the position of the concept of vulnerability and vulnerable individuals in the data protection law.
c) to ascertain the latest legal regulatory reformations in the e-commerce related areas.

4. The methodology of the research

The research methods used in this dissertation would be legal analysis and comparative research methods. As *John C. Reitz* mentioned, 'the comparative method' is to focus on the similarities and differences between the compared legal systems, but in assessing the significance of the differences, the comparativist must consider the possibility of functional equivalence. Comparative analysis is especially well-suited to draw conclusions about a) unique features of each legal system and/or b) commonality in how the law approaches the subject under study. By challenging the comparatist to explain the similarities and contrasts between legal systems or to consider their relevance for the cultures being studied, the comparative method has the ability to generate a more fascinating analysis.[16] In this dissertation, I utilized legal analysis and comparative research methods to explore the concept of vulnerability within consumer and data protection law. Specifically, I compared the legal frameworks of different jurisdictions to identify similarities and differences in how they address the protection of vulnerable individuals in online transactions. By examining case law, legislation, and scholarly works from various legal systems, I was able to provide a comprehensive analysis of the legal landscape surrounding vulnerability.

This dissertation would be based on the type of qualitative research, especially on the documentary/document analysis method. Because due to the documentary analysis method, it would be possible to review and analyse the work of lawyers, research reporters, legislation, and case law.[17] Document analysis is a methodical process for studying or evaluating documents, both printed and electronic (computer-based and Internet-based). Document analysis, like other qualitative research methodologies, requires the examination and interpretation of data to extract meaning, gain insight, and develop empirical knowledge. Skimming (a shallow examination), reading (a detailed examination), and interpretation are all parts of document analysis method.[18] A key component of my research involved document analysis, where I systematically reviewed and analysed legal documents such as legislation, case law, and scholarly articles. This

[16] J. C. Reitz, 'How to Do Comparative Law,' *The American Journal of Comparative Law*, vol.46/4, 1998, 620.
[17] K. Zweigert & H. Kötz, *Introduction to Comparative Law*, Oxford, Clarendon Press, 1998, 2-34.
[18] Glenn A. Bowen, 'Document Analysis as a Qualitative Research Method' *Qualitative Research Journal*, vol.9, no.2, 2009, 27-32.

method allowed me to extract meaningful insights and evidence to support my arguments regarding the definition and position of vulnerable individuals within consumer and data protection law. By closely examining these documents, I was able to identify trends, patterns, and emerging issues in the legal treatment of vulnerability.

Qualitative research produces words as data for analysis and sheds light on a variety of social life aspects. People's emotions, perspectives, and experiences are prioritised in qualitative research to investigate and comprehend 'the meaning individuals or groups ascribe to a social or human problem.' When statistical analysis or desk study research are unable to fully capture the perspective of a particular group of people, researchers who wish to delve further into an issue or topic may choose to utilise a qualitative approach. Ethnography and case studies are two of the most popular research approaches that can be used as part of qualitative research methodology. To understand the social phenomena that a group or organization represents, the case study approach refers to the collection and presentation of detailed information about a specific participant, small group, or organization, seen in a 'real-world' setting.[19] Only court decisions provide remarkably comprehensive and deep insights into the law, the actions of various participants, and the social environment in which they take place. Qualitative analysis methods are crucial for legal researchers as they examine the relationships between cases linked by previous rules.[20] To delve deeper into the social aspects of vulnerability within legal contexts, I employed qualitative research methodologies such as case studies. Through in-depth analysis of real-world cases, I was able to explore the experiences, perspectives, and emotions of individuals affected by consumer and data protection laws. This qualitative approach provided valuable insights into how vulnerable individuals navigate legal systems and interact with online transactions, enriching the overall understanding of vulnerability within legal frameworks..

The 'functional method' is occasionally referenced with the optimistic conclusion that, while concepts and processes may differ, most legal systems will eventually find common ground in the resolution of legal issues. According to *Ralf Michaels*, 'the functional method' is a triple misnomer, to put it briefly. Firstly, there are numerous functional methods rather than just one ('the'). Moreover, not all allegedly functional

[19] Kristina Simion, 'Practitioner's Guide: Qualitative and Quantitative Approaches to Rule of Law Research', INPROL—International Network to Promote the Rule of Law, 2016, 7-17.
[20] Katerina Linos & Melissa Carlson, 'Qualitative Methods for Law Review Writing', *The University of Chicago Law Review*, vol.84, 2017, 214.

approaches are really 'functional' at all. Finally, some initiatives that claim to be committed to this do not even stick to any 'noticeable methodology'. In fact, the term 'functionalism' is used in a variety of contexts to achieve a variety of objectives, including understanding the law, comparing (tertium comparationis), emphasising similarities (praesumptio similitudinis), constructing systems (such as 'legal families'), identifying the 'better law,' unifying the law, and critically evaluating the legal systems. This range of 'functional methods; emphasises how crucial the research question and purpose are in selecting the best comparative method. Essentially, what and how the researcher compares are determined by the research question(s) and interest. Functionalism examines how various civilizations handle real-world conflicts of interest under their respective legal frameworks. In its most basic form, the functional method compares solutions to real-world issues involving competing interests rather than primarily rules.[21] Finally, I applied the functional method to assess how different legal systems address conflicts of interest related to vulnerability. By focusing on practical solutions rather than abstract rules, I was able to identify commonalities and best practices across jurisdictions. This comparative approach facilitated a nuanced understanding of how legal frameworks adapt to emerging challenges in consumer and data protection law, contributing to the ongoing discourse on vulnerability and legal protection.

5. Contribution to scientific field

This dissertation's primary contribution consists of examining and distinguishing the concept of vulnerability and its legal implications from several legal perspectives, which have not yet been adequately studied on academic grounds. The success of this work lies in the ability to combine the concept of vulnerability from two very different legal disciplines - consumer and data protection law - which would help to understand this concept from various perspectives while keeping in mind its distinct qualities and characteristics. By viewing and comparing this concept from different legal disciplines, it would be more practical and understandable to draw a complete picture of vulnerability as a concept.

Most importantly, this study intends to add knowledge and practical value to the legal disciplines of consumer and data protection legislation, as well as to the field of e-

[21] M. Van Hoecke, 'Methodology of comparative legal research' *Law and Method*, 2015, 9.

commerce. Exploring this concept and providing a concrete perspective on it will benefit both consumers and data subjects, as well as be practical and useful to traders and data controllers in general. Additionally, there is a chance that our effort will make traders and data controllers in the future more cautious and aware when interacting with this concept and vulnerable individuals in general. This dissertation also draws the attention of EU legislators to the need to better assess and review the current position of vulnerabilities and vulnerable individuals in both the legal areas of consumer and data protection law.

6. The structure of the research work

In this dissertation, all work is summarized in 6 chapters. The dissertation began with an introduction, then the main chapters follow, and ends with a final chapter with research commentary in the conclusions.

In Chapter One, after the introduction, the focus is on the research questions, research objectives, research sources, methodology, contribution to the scientific field, research limitations, and research structure of the work.

In Chapter Two, the field of e-commerce will be addressed as a separate area of law with distinct features and structures. There will be some discussion of the benefits and drawbacks of e-commerce as a distinct field. In broad terms, numerous e-commerce categories will be explained depending on a variety of circumstances. Due to the availability of appropriate resources, the focus will be on the regulation of e-commerce from an EU perspective, in addition to the perspective of the numerous international organisations on the definition and importance of e-commerce.

Chapter Three will begin by examining the main consumer-related category of e-commerce, namely business-to-consumer (B2C) transactions. Following a quick introduction of the EU regulatory framework for consumer protection, the concept of average consumers will be redefined. Later, the notion of vulnerability and vulnerable consumers will be thoroughly addressed in terms of its definition and provisions in EU consumer protection law to determine if EU consumer law can adequately identify and protect vulnerable consumers in online transactions.

Chapter Four will provide a brief summary of how technology advancements have influenced the development of privacy and data protection law. Later, while determining the status of data subjects in exercising their rights when processing personal data in accordance with GDPR regulations, the various rights of data subjects with pertinent court

cases will be taken into consideration. To determine the extent to which EU data protection law can define and ensure adequate protection of vulnerable individuals during data processing, average and vulnerable individuals will be examined and analysed as the data subjects after the main provisions of the GDPR.

Chapter Five focuses on e-commerce security in general, with a particular emphasis on data processing security, network and communications security, and other significant regulatory developments in the EU. And the emphasis will be on determining to what extent existing security policies are adequate for providing a suitable environment for their users. The chapter's major section evaluates the present e-commerce strategy, particularly the DSM Strategy. Later, the approaches for regulating e-commerce-related fields will be explored, especially considering the recent digital transformation.

The connection between the chapters is reflected in the possibilities and prospects for online individuals to participate in the different legal dimensions simultaneously. When these individuals enter the online world of the Internet to browse, they become online users of that network. Especially when online users access certain websites, they must give or decline consent to the use of their personal data over the Internet. This is precisely the moment when the same online user, unknowingly and due to circumstances, becomes a data subject of personal data processing through the Internet. Later, the same online user, by purchasing or buying goods or services in shopping carts, becomes the online consumer. Therefore, despite the differences, it is possible to focus on online individuals by considering the unique characteristics and special features of the areas of e-commerce, consumer, and data protection law. And since an online individual can be involved in different legal disciplines as an online user, as an online consumer and as a data subject, these also impact their safety and security in all these areas. The same online individuals, especially the vulnerable individuals in these relations from the various legal disciplines, also form connecting chains between all chapters of the dissertation.

The last part of the dissertation is the conclusion of the research findings with some recommendations for future accomplishments in keeping the interest of online users, whether online consumers or data subjects at the highest level.

II) Scientific results and recommendations

Since one of the main rational motives for solving the research questions was the study of e-commerce, it can be said without exaggeration that e-commerce cannot be limited to one discipline, since it is characterized by a variety of options and infrastructure components supported by technologies. In order to explore the potential and future prospects of e-commerce, it is advisable to consider it as a separate discipline and not as a sub-area of e-business law. The final line is that whether it is online commerce or digital commerce, processes are the same in their fundamental operation and structure and should be regarded as terms that are commonly used interchangeably. Due to its distinct qualities as a multidisciplinary approach, e-commerce law has incorporated this potential into its systems and applications. All elements, especially e-commerce systems and e-commerce applications, must be integrated, interact and function simultaneously for the constant and consistent development of e-commerce in order to achieve the desired results and avoid unforeseen problems. The most recent regulatory changes in digital services and online marketplaces demonstrate the ongoing efforts of the e-commerce industry to keep up with the most recent internal market digital transformation. Therefore, e-commerce can be defined as online transactions and sales carried out through information technology networks using different devices and formats between different types of participants. Since e-commerce covers businesses, organisations, and individuals, it is logical to consider e-commerce as a separate field with several levels of interaction.

Since no two individuals are alike, they can be identified by a variety of traits, including age, gender, credulity, and physical or mental instability. These distinguishing features show that while not all people can be classified as normal or standard, some people can be excluded from the group. When connecting with others online, individuals with these typical traits could feel more susceptible and vulnerable. Since there wasn't a complete definition of the term vulnerability, it was required to search for one and evaluate the ones that academics have already put out. Here are some results of the research work based on the findings of the research questions:

1) To what extent can the EU define the concept of vulnerability and the position of vulnerable individuals in consumer protection law.

The EU has somehow managed to create a static fixed definition of the vulnerable consumer category, although it is only developed from the perspective of the UCPD. So, the vulnerable group of consumers is defined as a clearly identifiable group based on

mental or physical disability, age or credulity, and the trader can reasonably be expected to 'foresee their vulnerability'. Despite the EU's efforts to define vulnerable consumers, this definition lacks situational and inherent elements, which are, naturally, crucial components of different consumer groupings. Another factor behind this definition is that it does not accurately reflect the digital capabilities of vulnerable or online consumers, making it impossible to assess their current digital value in the online marketplace. As a result, consumer protection laws and policies that affecting vulnerable consumers do not apply to other consumer-related online industry practises, such as contractual relationships or dispute resolution circumstances.

The UCPD is no longer up to date to provide an adequate definition of the vulnerable consumer group that should be proportionate to the recent digital revolution, particularly by using the average consumer group as a benchmark for consumer protection law. For guidance that involves a vulnerable group of consumers, not only in commercial practices but also in other consumer-related industries, a consistent and coherent approach should be taken directly into account when formulating digital vulnerability criteria. Particularly in view of the explosive growth of information technology, the position and availability of the most vulnerable group of consumers must be adequately adjusted to the concerns of the modern DSM. As recommendations for the future, particularly for greater performance and realistic contribution, the legislators should identify the characteristics of particularly digitally vulnerable consumer groups and their tendency to be particularly vulnerable to particular commercial practises.

So, according to the legal framework of the EU consumer protection, it is recognized that the EU's consumer regulatory mechanisms are more effective at defining and protecting the typical average group of consumers, both in theory and in practice. It is practically very difficult for the vulnerable group of consumers to realise whether they require protection from unfair commercial practices, despite the existence of provisions for them in the EU consumer protection law. These vulnerable consumer groups will always require additional guidance and support in online transactions since they do not receive reliable information, or this is not achievable due to extrinsic and intrinsic reasons.

Based on the CRD and the UCPD, some recommendations should be considered to protect vulnerable individuals under the EU consumer protection law:

a) Provide clear and transparent information. Sellers and service providers should provide vulnerable consumers with clear and understandable information about their

products or services. This includes information about prices, terms and conditions, and any potential risks or side effects.

b) Avoid aggressive or misleading sales practices. Companies should not use misleading or aggressive sales tactics that take advantage of vulnerable consumers. This includes avoiding pressure selling, hidden fees or charges, and false claims about a product or service.

c) Ensure accessibility. Companies must ensure that their products and services are accessible to all consumers, regardless of their vulnerabilities and shortcomings. This includes providing information in alternative formats such as braille or audio and offering the assistance to consumers with disabilities.

d) Offer refunds or the right to cancel. Companies should offer refunds or the right to cancel for vulnerable consumers who may have made a purchase by mistake or who are experiencing financial hardship.

e) Provide proper customer service. Companies must provide adequate customer service to assist vulnerable consumers with any questions or concerns they may have regarding their purchase or service. This includes offering multiple customer support channels such as phone, email, and live chat.

2) To what extent can EU explain the concept of vulnerability and the position of the vulnerable individuals in the data protection law.

Since consumers and data subjects are in a weaker position in each of these areas due to their status, it is reasonable to put forward an average concept of the data subject as a starting point in data protection law similar to consumer protection law. The mention of vulnerable natural persons implies that the data controller may occasionally rely on non-vulnerable individuals as average or standard data subjects, even though the GDPR treats all data subjects equally and applies the data processing laws to all of them. Although data subjects are identified and identifiable persons in the GDPR, it is worth defining some standard concepts of data subjects for further processing of personal data. The requirement to identify the status of average data subjects is also driven by the significant role of the data controller in the power of imbalance resulting from information processing asymmetry. It is necessary to introduce a standard notion of the average data subject in data processing so that data subjects can more effectively exercise their rights in practice. The requirements of the GDPR are intended to preserve everyone’s privacy and rights, regardless of their unique features or circumstances, which may be one of the reasons why the concept of average data subjects has not been properly explored.

Thus, in general, the data protection law, in particular the GDPR, did not develop either the notion of an average data subject or the notion of a vulnerable data subject as a concept, but slightly referred to children as vulnerable natural persons. On the other hand, the absence of average data subjects in data protection regulation may also mean that vulnerable data persons remain unprotected against the background of average data subjects. Although the concept of vulnerability is inevitably present in data protection law, it is still not sufficiently recognized as a basis for defining the social differences of data subjects. It is possible to unleash the potential of the GDPR and secure the processing of personal data of various underprivileged data subjects by bringing the notion of vulnerability into data protection law, particularly in relation to data subjects. In the data processing, the category of children as vulnerable data subjects is referenced with features of parental consent and data controllers' information obligations. Data controllers, by analogy, cannot impose the same obligations on different groups of persons as vulnerable data subjects. Thus, it would be preferable if data controllers took extra precautions when processing the data of various groups of vulnerable data subjects. Therefore, if the data controller is aware that their products or services are used by (or targeted at) other vulnerable members of society, such as people with disabilities or people who might have difficulty accessing information, the data controller should also consider the vulnerabilities of such data subjects when deciding how to ensure that it complies with its transparency obligations regarding such data subjects. Additionally, data controllers must be aware of the nature, scope, and context of processing that could constitute serious risks to the rights and freedoms of data subjects at every stage of processing because they are responsible for the purpose and method of processing. As a result, in general, when processing data, and being responsible and accountable, the data controllers should refrain from preying on the weaknesses of the vulnerable data subjects.

Based on the GDPR, here are a few more recommendations for protecting vulnerable individuals under data protection law:

a) Get informed consent. Companies must obtain the informed consent of vulnerable individuals before collecting, processing or sharing their personal data. This means providing clear and understandable information about the purpose of data processing, the identity of the data controller, and any potential risks or consequences of data processing.

b) Provide access and control to data. Companies must provide vulnerable individuals with access to their personal data and the ability to control how their data is

used. This includes the right to request the erasure of data, data portability and restrictions on data processing.

c) Ensure security of data. Companies must ensure the security of the personal data of vulnerable individuals, including the adoption of appropriate technical and organisational measures to protect against unauthorized access, disclosure, or loss.

d) Provide transparency of processing. Companies should provide vulnerable individuals with transparent information about their data processing activities, including the categories of personal data collected, the purposes of the processing and the recipients of personal data.

e) Monitor and report data breaches. Companies should monitor data breaches and report them to the relevant authorities and the affected vulnerable individuals. This includes providing clear and understandable information about the nature and extent of the violation, as well as the potential risks or consequences for affected vulnerable individuals.

3) To what extent can EU e-commerce deal with recent regulatory issues?

As a result of technological innovations and emerging digital market trends, the EU is unavoidably going through a digital revolution. The epidemic and the economic crisis have hastened the digitalisation of the EU's society and economy along with them. If the EU is to maintain its position as a market leader in the digital sphere, strong and innovative measures by MS are also required. A brilliant model for the EU's approach to strengthening the sovereign single market, based on common EU values and principles, is the DSM Strategy. The DSM strategy will continue to prioritize fulfilling the needs of EU citizens, as it is based on common values and principles. The DGA and the proposed Data Act, which are both components of the European Data Strategy, indicate a bright future for building and enhancing the EU's single market for data space. The DMA and the DSA represent additional cutting-edge initiatives to close the digital divide and bring Europe into the digital era. AI is ushering in a new era in the digital sector, and new policies and frameworks like the AI Act and the AIL Directive are required to keep the EU at the forefront of the digital economy.

The EU digital industry usually tries to keep a close eye on modern technologies and digital advances. Accordingly, based on the most recent proposed legislative acts and directives, it is predicted that the EU is currently on the verge of a disconnected and complex digital review and transformation of the legal frameworks. It also shows how urgently the EU requires these changes and reforms to keep up with its sizable regional

rivals on the global stage and remain one of the key hubs of technology innovation. Regardless of how different and sometimes even unrelated the reasons and explanations for these legislative reforms may be, the desire and necessity for these changes in the digital economy must come before any other concerns. As shown by Europe's Digital Decade and its digital ambitions for 2030, the EU must update its digital regulatory legislative frameworks to establish a human-centric, trustworthy, and sustainable environment for all stakeholders. Given the capitalist nature of the digital world, it is not surprising that the EU is determined to stay up with these digital races by creating its DSM Strategy at the highest level. Therefore, the EU's efforts to keep track of the most recent digital revolutions and changes are admirable and appropriate in terms of maintaining the EU's position as an industry leader in this regard. These legal updates for the digital age will also help the EU prepare for potential future challenges and ensure that everyone who uses the Internet feels safe and secure. Still, the EU has many adjustments to come in the form of proposed and submitted regulations, evaluation reports and stakeholder workshops on the implementation and application of adopted regulations, directives, and acts. The EU would have the chance to spot any errors, inconsistencies or demands from valid stakeholders regarding the future execution of these legal acts between the proposed legal acts and their implementation deadlines. Furthermore, there's always a potential that the proposed legislations will one day experience the same 'Brussels Effect' as the GDPR, which was approved not just in the EU, but also internationally. The 'Brussels Effect' would highlight the EU's strategic requirements for the DSM and the global regulatory authority for enacting further legislative reforms.

III) The list of the author's publications written within the topic of the dissertation

1. Narmin Miriyeva, 'European Payments in the Digital Age' ELTE Law Journal, vol:2, (2022), pp. 35-60., 26 p.

2. Narmin Miriyeva, 'The Legal Impact of COVID-19 on Online Consumer Behavior' in: Ristivojević, Branislav (eds.) Harmonizaciǰa srpskog i mađarskog prava sa pravom Evropske uniǰe = A szerb és a magyar jog harmonizációja az Európai Unió jogával = Harmonisation of Serbian and Hungarian Law with the European Union Law:ТематСки зборник = Tematikus tanulmánykötet = Thematic collection of papers Novi Sad, Srbija : Újvidéki Jogtudományi Kar, Kiadói Központ (2022), pp. 405-424. , 11 p.

3. Narmin Miriyeva, 'E-Commerce in the Time of Covid-19' in: Hajdu, Gábor (eds.) Rendkívüli helyzetek és jog: Kalandozások a jog peremvidékén a COVID-19 apropóján Szeged, Hungary: Iurisperitus Bt. (2021) 172 p., pp. 93-109, 17 p.

4. Narmin Miriyeva, 'Security in Electronic Commerce and Online Payments' In: Cebeci, Kemal; Silva, Joaquim Ramos; Focacci, Antonio; Goyal, Tanu M. (eds.) Conference proceedings Rome 2020, Italy: Masters International Consultancy Research and Publishing (MIRDEC Publishing) (2020), pp. 17-28, 12 p.

5. Narmin Miriyeva, 'Free Trade and E-Commerce: Is there any influence on each other?' Annals of the West University of Timisoara-Law Series., (2021) pp.154-167, 14 p.

6. Narmin Miriyeva, 'The Impact of Big Data on Business and Electronic Commerce' in IAI Academic Conference Proceedings, Skopje, (2020) pp. 46-53, 8 p.

7. Narmin Miriyeva, 'Ethics in E-Commerce: Is There a Unique Ethics in E-Commerce?' in IAI Academic Conference Proceedings, Skopje, (2019) pp. 84-94, 11 p.

8. Narmin Miriyeva, 'The mobile commerce as the next generation of e-commerce' in Forum: Publicationes Doctorandorum Juridicorum, vol.9, (2019), pp. 69-85, 17 p.

9. Narmin Miriyeva, 'Literature Review of Electronic Commerce Security and it's Regulation' in Comparative Law Working Papers, (2019), vol.3: 1 Paper:7, 12 p.