Vilnius University Faculty of Law
Department of Public Law

Yelyzaveta Nalkovska
II study year, International and European Law Programme Student

Master's Thesis

Restrictions of the Right to Conduct Business in the Digital Domain in the Interests of Protecting Other Human Rights
Teisės užsiimti verslu skaitmeninėje aplinkoje ribojimas dėl kitų žmogaus teisių apsaugos interesų

Supervisor: assoc. prof. dr. Vygantė Milašiūtė
Reviewer: prof. dr. Neringa Gaubienė

Vilnius
2023

ABSTRACT AND KEYWORDS

The master's thesis analyzes personal (individual) digital human rights, the violation of which restricts the right to conduct business in the digital sphere. The author characterizes the rules for observing digital human rights through mandatory registration and licensing of digital enterprises, as well as compliance with the GDPR. The issues of legal and digital liability, application of administrative and financial sanctions for violation of rights are investigated based on the experience of European countries.

Keywords: rights protection, personal data, GDPR, digital enterprises, user, license, liability.

Magistro darbe analizuojamos asmeninės (individualios) skaitmeninės žmogaus teisės, kurių pažeidimas riboja teisę užsiimti verslu skaitmeninėje erdvėje. Autorė apibūdina skaitmeninių žmogaus teisių laikymosi taisykles, taikant privalomą skaitmeninių įmonių registraciją ir licencijavimą, taip pat BDAR laikymąsi. Teisinės ir skaitmeninės atsakomybės, administracinių ir finansinių sankcijų už teisių pažeidimus taikymo klausimai nagrinėjami remiantis Europos šalių patirtimi.

Pagrindiniai žodžiai: teisių apsauga, asmens duomenys, BDAR, skaitmeninės įmonės, naudotojas, licencija, atsakomybė.

TABLE OF CONTENTS

INTRODUCTION……...……...2
1. PART I
1.1. Importance of licensing business in the digital sphere and registration of digital enterprises as an important element of human rights protection……..5
1.1.1. Protection of fundamental human rights in the digital space…….…….....5
1.1.2. Mandatory business licensing in the digital sphere today……..……..…....9
1.1.3. The importance of registration processes for digital enterprises for the proper protection of human rights……...……...16
2. PART II
2.1. Study of human rights protection mechanisms in digital enterprises…….……..20
2.1.1. Content monitoring mechanisms implemented by digital enterprises as one of the elements of human rights protection…….……..…..……20
2.1.2. Implementation of human rights protection in digital enterprises by European legislation….....24
3. PART III
3.1. Implementation of sanctions and other types of liability for digital enterprises……...…….……..29
3.1.1. Establishment of administrative and financial sanctions for digital enterprises in case of human rights violations……..……29
3.2.1. Determining the types of legal liability for digital enterprises that violate human rights on a regular basis……..41
CONCLUSIONS…….……..……...…….…...50
LIST OF REFERENCES……..…..….53
SUMMARY …….…..…….…….……...60
SUMMARY (IN LITHUANIAN)…..…….…..…….……61

INTRODUCTION

Today, digital technologies are constantly evolving and the ways in which they are used are reflected in absolutely all areas of our society: education, healthcare, various types of industry and business, government activities, etc.

One of the important factors that accelerated the development of digital technologies and opened up the field of remote management is the COVID-19 pandemic, as lockdown conditions, restrictions on the movement of individuals, allowed many segments of the population to function and operate remotely for a long time.

However, despite the positive developments in the content of digitalization, there are a number of specific problems, including the increasing inequalities caused by the digital divide, the emergence of fair competition in online markets, privacy and consumer protection issues in the field of digital security.

When analyzing these factors and problems, it is important to note that international norms and principles of the United Nations on human and business rights, which can and usually are violated in the digital environment, are of particular importance and require appropriate protection.

For example, the UN Guiding Principles on Business and Human Rights include:

1) the obligation of the respective state to protect human rights from violations by third parties, including businesses;

2) the duty of business to respect human rights, which should be manifested in due diligence regarding the possible negative impact of a particular business activity;

3) the obligation to ensure the effectiveness of judicial, state, extrajudicial and non-state remedies.

The relevance and novelty of this study is the active manifestation and realization of digital rights by society, the opening of digital businesses, the transition of society to an electronic mode, the active use of artificial intelligence, and so on. The above has significantly increased the level of violations of digital human rights, the protection of which is currently well regulated in the EU and its Member States.

In this work, I investigate the mandatory nature of business licensing in the digital sphere and the importance of registration processes, and point out the need to regulate registration processes by legislating them and having them duly formalized as a mandatory procedure. I examine not only the types of legal liability in the form of administrative and

financial sanctions, but also the types of digital legal liability in the field of digital technologies.

The subject of the study is restrictions on the right to conduct business in the digital sphere in the interests of human rights protection.

The object of the study is the social, legal and administrative relations arising from the protection of human rights in the context of doing business in the digital sphere and their restriction.

The purpose of the study is to identify the specifics of human rights in the digital space, the process of their protection and the types of liability for their violation. In accordance with the purpose, the author of the study has the following tasks:

1) to reveal the protection of fundamental human rights in the digital space;

2) to determine the mandatory nature of business licensing in the digital sphere today;

3) to explore the importance of registration processes for digital enterprises for the proper protection of human rights;

4) to characterize the implementation of privacy and security of personal data of consumers by digital enterprises;

5) to determine the process of implementation of human rights protection in digital enterprises by European legislation;

6) to identify administrative and financial sanctions for digital enterprises in case of human rights violations;

7) determine the types of legal liability for digital enterprises that violate human rights on a regular basis.

The methodological basis of the work includes general scientific and special methods of scientific knowledge as follows: comparative legal method - to establish the concepts of different scientific approaches; the method of distinction from the concrete to the abstract - for analyzing scientific approaches, identifying features, and developing scientific thought; the method of system analysis for building a logical research; the method of analysis and synthesis - to determine the importance of registration processes for digital enterprises, for the proper protection of human rights, to characterize the process of implementation of privacy and security of personal data of consumers by digital enterprises; method of legal analysis - to reveal the content of the protection of fundamental human rights in the digital space; the method of legal reality - to determine whether licensing of business in the digital sphere is mandatory today, to determine the process of implementation of human rights protection in a digital enterprise by European legislation; systemic method - to determine the

types of legal liability for digital enterprises that violate human rights on a regular basis, to establish administrative and financial sanctions for digital enterprises in case of human rights violations.

PART I

1.1. Importance of licensing business in the digital sphere and registration of digital enterprises as an important element of human rights protection

1.1.1. Protection of fundamental human rights in the digital space

Human rights have been conceptualized and regulated in response to the historical experience of violations of human freedom by the state and its bodies (Khrystova, 2018, p. 130-135).

The central place in the very idea of human rights protection is occupied by the state's obligations to prohibit interference in the sphere of individual freedom, requirements for respect for human rights, their guarantee and provision, protection and promotion of their realization (Uvarova, 2019, p. 8).

These obligations of the state, by their nature, have an international and constitutional nature, because their legal basis is international human rights law and the constitutional legal order, namely the norms and principles of constitutional law. (Hristova, 2018, p. 433).

When analyzing these legal norms, it is important to note the concept of international human rights standards. I support the position of O. Uvarov regarding the definition of the above concept as universally recognized norms and principles of international law which at the universal level affirm the status of a person as the highest social value and, accordingly, establish a list of fundamental rights and freedoms, the obligation of states to respect them, as well as the limits of possible or permissible restrictions on them (Uvarova, 2019, p. 9).

At the same time, it is important to note that the main documents that enshrine international standards on fundamental human rights and their protection include:

1) The Universal Declaration of Human Rights (1948), (Universal Declaration of Human Rights…);

2) Document of the Copenhagen Conference on the Human Dimension of the CSCE (1990), (Document of the Copenhagen Meeting - Conference on the Human Dimension of the CSCE…);

3) Outcome Document of the Vienna Meeting of Representatives of the participating States, (Final Document of the Vienna Meeting of the Representatives…);

4) International Covenant on Economic, Social and Cultural Rights (1966), (International Covenant on Economic, Social and Cultural Rights…);

5) European Social Standard (1961), (European social standard…);

6) Final Act of the Conference on Security and Cooperation in Europe (1975), (Final Act of the Conference on Security and Cooperation in Europe…);

7) The European Convention for the Protection of Human Rights and Fundamental Freedoms with Protocols (1950), (Convention for the Protection of Human Rights and Fundamental Freedoms…);

8) Conference on Security and Cooperation in Europe (1989), (Conference on Security and Cooperation in Europe….);

9) International Covenant on Civil and Political Rights (1966), (International Covenant on Civil and Political Rights…);

However, not only the binding norms mentioned above include international human rights standards, but also soft law norms, as opposed to contractual norms. These standards are used to fill in gaps in the law, to characterize and interpret norms, and to directly contribute to their development. At the same time, they play one of the most important roles in the process of implementation of international law (Prof. V.V. Phillipov, 2011, p.17).

The content and text of the so-called soft law is not legally binding as most adhere to the principles and norms reflected in international documents or agreements that have a recognized authoritative value as a vision of the aspirations, intentions and positions of international organizations and their bodies.

States themselves and their agencies may have recourse to soft law for the following reasons:

- when they are unable or unwilling to adopt measures of a more stringent nature, it is advisable to outline future directions and fill or remove gaps in the international legal order;

- in cases where state authorities have concluded that legally binding mechanisms are not the best tool to address the immediate problem;

- in cases where the state gains a political impetus to avoid additional binding measures (O'Brien, 2018).

International law on human rights and their protection plays an important role at the national level and directly affects the domestic legislation of the European Union (EU) member states. Therefore, direct international treaties on the subject matter impose obligations on the Member States, as this has important consequences for all national authorities (legislative, executive and judicial).

Thus, human rights in today's realities should be considered certain requirements addressed to states. This understanding is fully consistent with the classical structure of

understanding human rights, which includes the addressee (bearer of obligations), the bearer of the right and the subject of the right (requirements), (Alexi, 2008, p. 174).

It should be further noted that not only the state is the main actor in the protection of human rights. Gradually, the framework of the classical concepts of human rights and their protection has been established in international law through the recognition of businesses as bearers of human rights obligations and their protection.

Turning to the analysis of the protection of rights violated in the digital space, it is worth noting that the rapid development of technology, changes in old legal relations and the emergence of new forms of business and economic activity, asymmetry of information and the increase in the online life of individuals raise the issue of conceptual law in terms of its legal regulation and legal practice.

In other words, the most important values for a person are freedom, the rule of law and justice. And if his or her rights are under threat - their protection requires consideration, changes and implementation of new legal instruments.

Thus, in order to analyze the protection of human rights in the digital space, I believe it is important to define the concept of digital human rights. Today, there are two understandings of this aspect. While the first understanding refers to human rights, the protection and realization of which are closely related to the use of online components and digital tools, the second refers to those human rights that arise in the course of activity and claim to be fundamental and fundamental in the digital space.

Thus, the list of digital human rights should include the following fundamental rights, namely the right to information, privacy, participation in public affairs, freedom of expression and opinion, the right to be forgotten and, accordingly, to anonymity, and the general right to the Internet (Right to privacy..., 2003, p. 19). One of the most important issues of human rights protection in the digital space is the protection of information about private life (Milanovic, 2015, p. 64).

This is due to the fact that in the digital environment information about personal and private life is disseminated and threatened quite often. As is well known, the disclosure of private or personal information of a person can affect not only the moral state of such a victim, but also the position of a person in society.

Also, despite the fact that digital space is increasingly filling the life of society today, international civil society organizations emphasize that the Internet is the space that threatens human rights defenders. This is because society is increasingly exposed to attacks and abuse by private actors simply because of their activities on the Internet in support of human rights.

In the following, I propose to consider the protection of digital human rights, which are most susceptible to violations and threats in the current context.

1. The right to be forgotten. This right allows a person to demand that the relevant entity, under appropriate conditions, remove his or her personal data from public access through search engines, i.e., to remove those links that, in the opinion of a particular person, may harm the latter (Derevyanko, 2023, p. 55).

Today, the right to be forgotten is reflected in some decisions of the Court of Justice of the European Union (hereinafter referred to as the EU Court) that directly relate to the protection of this right. The most appropriate example would be the case of Google v. CNIL" case of the French regulator on the possibility of covering the global nature of the right to be forgotten in connection with the problems that arose with this multinational corporation outside the territorial scope of the EU. Analyzing this case, I came to the conclusion that the CJEU found that the corporation was not required to erase data outside the EU and remove digital traces from all versions and search systems, based on the fact that citizens of EU member states have a legal right to be forgotten, but it is not absolute and must be properly balanced within the EU. However, at the same time, the EU Court of Justice provided recommendations on the possible erasure of all data to the national courts of EU member states (Google v. CNIL: The Territorial…).

It follows from the above that Google processes special categories of private data of individuals, and if required by the national courts of the EU member states, in each individual case, this corporation must prove that the processing and non-deletion of data is of significant and essential interest to society.

Privacy (confidentiality) is the most important human right that needs to be protected in today's environment, as new technologies, tools and communications complicate privacy issues.

A relevant decision on the protection of privacy is the decision of the European Court of Human Rights (hereinafter referred to as the ECHR) in the case of Bărbulescu v. Romania. This judgment declared the limits of surveillance of a particular employee at his or her workplace using the latest communication channels to be limited. This proves that judicial practice in resolving a particular conflict will be quite dynamic and controversial (Bărbulescu v. Romania [2017] ECHR 754…).

In general, the interference with a person's private life in today's realities is quite common. Unfortunately, their nature allows them to be invisible, as a person does not always pay attention to the means of surveillance when in a particular state of publicity.

2. Freedom of expression and speech. The protection of this right is reflected in the balance of respect for freedom of expression of privacy and views, counteraction to hate speech, protection of honor, reputation, dignity, data, and legitimate interests.

For example, the balancing of fundamental rights today should not only strike a balance between individual privacy and the freedom of the media at the national level, but also take into account different interpretations of the content and scope of these rights, if, for example, a certain conflict concerns the digital environment or the use of digital tools. For instance, if there is a conflict between the right to protect private data and the right of the media to process such data, the importance of freedom of expression and the role of the media for freedom of information is taken into account. However, at the same time, the issue of protection against excessive coverage of personal or private data of a person is determined (Razmetayeva, 2020, p. 22).

At the same time, international law on human rights and their protection is ensured not only by joint international and EU law, but also by the domestic legislation of each individual EU member state.

In today's realities, human rights should be considered as requirements addressed to both the state and its relevant bodies and enterprises, and, in accordance with the issue under study, to digital enterprises.

Thus, in the digital space, it is digital rights, the realization and protection of which are closely related to the use of online components and digital tools, as well as those that arise in the course of digital activities and claim to be fundamental in the digital space, that need to be protected first.

The list of digital human rights includes the following fundamental rights, namely the right to information, privacy, participation in public affairs, freedom of expression and opinion, the right to be forgotten and, accordingly, anonymity, and the general right to the Internet. In addition, the analysis of the ECHR and the EU Court of Justice case law revealed that each individual case is considered separately and all factors are weighed for a full and lawful resolution of the case on the merits.

1.1.2. Mandatory business licensing in the digital sphere today

The digital enterprises, both large and small, must adapt to the standards of today. This is quite a challenge for them but, at the same time, new opportunities are opening up for

enterprises, namely, to achieve better efficiency and increase their competitiveness in the digital market.

Digitalization in companies is the replacement of conventional production and business processes with their digital equivalents, monetization of existing data. Today, it is an important element of market success and often even one of the main conditions for maintaining positions in the digital space.

It is important to note that the digitalization of processes is relevant not only at the level of individual enterprises, as entire industries choose this path of development as the only way to meet the rapidly changing conditions of the world around them. As a result, the digital transformation of industry, retail, the public sector, and other areas is already changing the lives of every person and every company.

Digital technologies make it possible to organize the most personalized interaction, which is preferred by most customers. Digital communication channels, omnichannel, artificial intelligence, and robotics are already part of our daily lives. For example, the digital transformation of banks cannot do without chatbots, and the pharmaceutical industry actively uses modern mobile devices in its work.

The introduction of advanced and new technologies transforms traditional economic processes by opening new market niches, improving the quality, speed and availability of services, changing the market environment, changing the way of doing business, making a profit from it and adjusting production to the current needs and tastes of a particular consumer. At the same time, in order to form a digital economy that will meet the current realities of today, it is necessary to achieve an active dialogue between business and law, government and society, by focusing the state's efforts on developing and creating effective legal regulation using the latest technologies, as well as eliminating problems that create obstacles to business development, such as minimizing burdensome procedures and rules that are unnecessary and eliminating bureaucratic burdens.

Due to the change in the regulatory paradigm, most countries in the world are searching for and subsequently implementing the experience of successful legal instruments and practices to improve the national regulatory system. This will make the system consistent, more flexible and responsive to market and technological changes. It will help to reaffirm their credibility and enjoy significant trust from the business community.

The issues of creating a favorable regulatory environment are still relevant today, as despite the implementation, streamlining and updating of the legal framework, harmonization

of the development of public relations, there are risks of violation of rights in the digital sphere.

When analyzing the aspects of improving legal regulation in the area under study, it is important to reveal the content, concepts and clearly outline the field with possible problems and adapt it to the new and modern technological reality by adopting innovative regulatory decisions.

In the course of analyzing the concepts established in legal science I have defined that within the framework of the general theory of law, legal regulation is the influence of law on various relations in society. At the same time, many scholars understand legal regulation as an effective regulatory and organizational impact on the relevant social relations through the system of legal means.

It is important to note that the most important social relations may also be subject to legal regulation. For example, with regard to economic relations, their legal regulation is related to the implementation of economic activities and is reflected in a set of measures to apply mandatory requirements to business entities by the state, appropriate measures to influence those who violate the requirements, as well as supervisory, notification and permitting procedures.

From the content of these concepts, it is possible to determine the sequence of elements, namely:

- establishment of mandatory rules, standards and, of course, requirements;
- control over their implementation or compliance;
- implementation of liability measures (if the requirements are violated).

The set of requirements that have the status of mandatory is the basis for regulating legal relations in the economic sphere and their violation leads to negative consequences for business and liability of the controlling entity. Additionally, it may further affect the security in the field of regulated public relations.

Considering in more detail the legal framework for the protection of human rights through the prism of licensing digital enterprises, the first to be noted are the UN norms, namely the "Convention for the Protection of Human Rights and Fundamental Freedoms", in which:

- Art. 8 provides for the right to respect for private and family life, as most digital enterprises often require the input of personal data, which allows the state to request a license;

- Art. 10 provides for freedom of expression, which can be more applicable to digital enterprises that disseminate certain information, and the state can also require a license for such enterprises (Convention for the Protection of Human Rights and Fundamental Freedoms…).

The foregoing allows me to conclude that the qualitative and rational construction of a system of mandatory requirements that are understandable to both business and regulatory authorities is the basis for effective legal regulation of economic activity in the digital reality.

As for the protection of human rights through the prism of licensing of digital enterprises this protection is realized through the state, namely its initiative and warning to digital enterprises that collect or disseminate certain information, which can further protect people's right to privacy and freedom of expression (however, it should be borne in mind that freedom of expression is a rather specific issue and in most cases countries can restrict this issue by national law for the purpose of protecting their own interests). Therefore the requirements should be appropriate, feasible, clear and reasonable, in line with the level of development of digital technologies, and in line with the needs and principles of a market economy. At the same time, it is important to note that the relevance of digital rights, rather than general human rights, is accompanied by the fact that today the world's population spends more and more time using digital technologies, the Internet and online media.

The digital transformation of the economy and business activities in particular has suffered to a greater extent from the instability of legal regulation, since the fullest disclosure of the potential of digital technologies is ensured primarily through their active use in all aspects of business: processes, products, services and decision-making approaches (Economic Commission for Latin America and the Caribbean…) The Economic Commission for Latin America and the Caribbean notes is quite significant for the issue under study, as it implies that the emergence of transformations of their own capabilities in most enterprises and the transition from physical to digital tasks is not easy, as it requires large physical and economic needs that not everyone can afford. However, it should be noted that there are certain contradictions in this opinion regarding the instability of legal regulation, which is caused by constant changes and improvements in the digital sphere.

Considering this contradiction through the prism of digital licensing, legal regulation also remains quite unstable, as the digital sphere is not limited to national borders, which leads to adaptation to international standards, rapid change in the digital sphere, where each situation needs to be considered separately, and most countries try to group them in one law and further improve it, which does not allow for full consideration of others.

In addition, it is important to mention that a large number of areas of social relations, within which types of supervision (control) and mandatory requirements are organized into certain groups, are dispersed in different regulatory sources. In some cases, many requirements are contradictory or duplicate each other, sometimes even redundant, making it impossible to create an exhaustive list, and for controlled entities it is difficult to understand what exactly will be subject to inspection. The situation is also complicated by the fact that traditional approaches to regulating objective reasons have exhausted their potential resources, while the latest regulatory technologies have insufficient methodological and descriptive basis and are not sufficiently adapted to existing institutions and the implementation of real legal relations.

Analyzing the legal framework, namely Directive 2000/31/EC of June 08, 2000, in particular the Directive on e-commerce, which reflects the rules of the obligation to license an enterprise in the digital space:

- according to Art. 5, the service provider is obliged to provide information for quick communication with him;

- according to Art. 6, the provider must comply with the rules on contracts that allow for the withdrawal from them within a certain period of time;

- according to Article 10, the supplier must comply with the transparency of digital commerce (Case C-298/07: Judgment of the Court (Fourth Chamber)…).

Next, it is important to note the Directive on Copyright in the Digital Single Market (2019/790/EU), where special attention should be paid to:

- Art. 2, which provides that authors may prohibit or authorize the use of their works;

- Art. 3, which provides that authors have the right to grant licenses to use their works;

- Art. 15, which provides that a Member State has the right to require a digital enterprise to record proof of an agreement to use an author's work;

- Art. 17, which provides that a Member State has the right to require a digital enterprise to personally control and monitor the information that is uploaded;

- Article 18 provides that a Member State has the right to demand from a digital enterprise to receive information about the persons who have downloaded the information (Directive (EU) 2019/790 of the European Parliament and of the Council …).

It is also worth mentioning the Electronic Communications Directive (2002/58/EC), namely:

- Art. 5, which provides for the requirement to provide users of digital enterprises with information about their rights and obligations (e.g., the right to privacy);

- Art. 6, which provides for the protection and confidentiality of user communications;

- Art. 8, which provides for the protection of minors from harmful content.

Thus, the above provisions of the Directives reflect the importance of a license for digital enterprises, which, in the course of their activities, fulfill one of their direct responsibilities - to protect human rights.

For instance, using the example of the Federal Republic of Germany (hereinafter referred to as Germany), I propose to consider the specifics of the rights and obligations regarding the licensing of a digital enterprise.

First of all, Germany has a variety of digital licenses covering different types of digital content, ranging from software licenses to music and image licenses. In other words, there is a wide range of digital licenses in this country that can be used for different purposes.

Digital licenses have different forms and for different types of digital content, the most common types of digital licenses in Germany include:

1) Software licenses. The content of this license is manifested in the essence of the agreement between software developers and users, which allow the latter to use certain software programs on their devices. Depending on the agreement, software licenses may include various rights of use, such as perpetual, time-limited, use on a specific device, or use for a specific purpose.

2) Music licenses. The content of this license is an agreement between music publishers, music studios or performers and users that allows users to use music in a certain way. The rights of use may vary depending on the agreement, for example, the right to broadcast, download or share music.

3) Image licenses are agreements between image agencies or image rights holders and users that allow users to use images in a certain way. The rights of use may vary depending on the agreement, for example, the right to use images for a limited time, size or type of use (The new digital edge: Rethinking…).

There are also other types of digital licenses, such as license agreements for e-books, videos, or games. Each type of digital license has its own specific terms of use and restrictions depending on the specific agreement.

Digital licenses are governed by various legal frameworks in Germany, and the key legal principles relating to digital licenses include:

a) The Copyright Act (UrhG) regulates the legal relationship between authors and users of protected works. It protects authors against unauthorized use of their works and guarantees them the right to compensation. Digital licenses are usually regulated by the Copyright Act

and must comply with the provisions of the law (Gesetz über Urheberrecht und verwandte Schutzrechte…).

b) Contract law. Digital licenses are governed by contracts between rights holders and users. Contract law regulates legal relations between the parties and ensures compliance with contractual agreements. Contractual terms and conditions must be clear and unambiguous to create a legally sound basis. It is important that users carefully read the terms of a digital license before accepting it (Vertragsrecht für Nichtjuristen...).

c) The Data Protection Law - regulates the processing of personal data. In many cases, users are required to provide personal information in order to purchase or use digital licenses. The processing of personal data by the copyright holder must comply with the provisions of data protection law. Therefore, users should always check how their personal data is stored, processed, and made available (EU GDPR).

Thus, when analyzing and issuing a digital license, it is important to note:

1) the subject matter of the agreement, which describes its digital content (software, images or music). This is necessary for users to choose the right license.

2) the scope of use, which describes how the digital content is to be used. This can include various restrictions and conditions, such as the number of devices on which the digital content can be used or the purpose of use.

3) license duration, which indicates the duration of the use rights. This can be a time-limited or perpetual license. For example, a time-limited license can be valid for a certain period of time or a certain number of uses.

4) commission - describes the price that the user must pay for the use of digital content (one-time commission or periodic payments). The amount of the commission depends on various factors (the amount of use or the duration of the license).

5) liability and warranty - describe the legal obligations of the parties to the contract. For example, rights holders can be held liable if digital content does not work as agreed. This ensures that users can expect a certain quality of digital content.

Considering the above, it can be concluded that in order to guarantee users their digital rights, it is important to comply with legal obligations when purchasing a license. At the same time, many EU member states have already implemented improvements in legal regulation, i.e., old and inappropriate acts are being repealed and new timely ones are being introduced. Thus, in ensuring legal stability, it is important to take a comprehensive approach, including the introduction of a comprehensive, full-fledged digital licensing regulation system.

The above also allows me to note that licensing of the digital sphere is quite significant in today's conditions, as it allows protecting consumers from fraud, ensuring transparency to all participants in the digital space, and helping to combat criminal and illegal content in the digital sphere.

However, it is also necessary to note the negative aspects of such activities, which are expressed by the fact that many digital spheres are not intended to earn large amounts of money, but are only used as an information base, increased costs and a large number of bureaucratic actions for licensing may force people to refuse to sell in the digital sphere, and inefficiency due to the rapidly changing digital sphere can be a separate point. Thus, digital licensing of businesses plays an important role in the human rights protection system. To date, all EU member states have brought their national legislation in line with the comprehensive, full-fledged system of regulating digital licensing and protecting human rights from the state. The main components of a license, which are necessary to guarantee users their digital rights, include legal obligations when purchasing a license: the subject of the contract, the scope of use, the duration of the license, the fee, liability and warranty. From my point of view, no improvements to the licensing system are needed today.

1.1.3. The importance of registration processes for digital enterprises for the proper protection of human rights

Registration processes of digital enterprises play an important role in the human rights protection system, as the process of acquiring the right to engage in digital business activities requires clear regulations and compliance with the relevant rights and obligations. The country is interested in regulating the registers of companies and entities engaged in both business and digital enterprise activities, since the act of registration and its publication can influence legal transactions and enter into legal relations with third parties.

For legal security purposes, it is also very important that all parties to legal relations are familiar with the basic data of digital business entities, and this can only be achieved through the use of digital technologies or online availability of such data. However, in recent years, this procedure has been supplemented by the possibility of electronic registration of business entities. Historically, the registration of business entities arose almost simultaneously with the need to organize activities in one of the established forms of business entities.

The Commercial Code, adopted by Milos Obrenović I in 1861, also contained provisions on the obligation of every trader, whether working alone or in partnership, to

report the company under which he wanted to operate to a certain commercial court. In addition, the trader was obliged to publish his company and shop in the official newspaper, together with the approval he received from the court to carry out the declared work. Also, when the merchant carried out his direct activities, he had to keep reports and send them to the commercial court (Miloš Obrenović…).

For example, the Republic of Croatia had a Commercial Law, i.e., legal article XVII of 1874, which was territorially applicable in Croatia and Slavonia. This law provided for mandatory registration, which was carried out by commercial courts in the form of a special book. It also determined the publicity of the register, which was of two types, i.e. one was kept for traders, which would correspond to today's idea of entrepreneurs, and the other for companies.

At the same time, the company registration system was introduced in the UK in 1844. Australia, as a British colony, also received its own legal legislation in the 19th century. An important document of business registration is the Directive on the establishment of a central company register throughout the European Union, which was adopted by the European Parliament in 2012, and which had to be ratified and implemented by the member states by July 7, 2014.

The aforementioned Directive became invalid in 2017 as a result of the newly adopted Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017, which in its content relates to certain aspects of company law, provides for possible cross-border access to business information about companies, including their branches established in other EU states. This can be greatly enhanced by the mandatory participation of absolutely all EU member states involved in ensuring electronic communication between the relevant registers, transfer of information to direct users in a standardized manner, and compatible technologies using identical content within the EU. This interoperability of registers is ensured by the national registers of the EU states that provide the relevant services and are the European central platform and its interface.

The content of the platform itself should be a centralized set with the use of information technology capabilities that form a common interface during integration. All national registries, in turn, should use this interface. At the same time, it should provide services for the formation of the interface through the portal, which is a European electronic access point and additional points for EU states. The platform should also explore how registries can be combined, but not as a third-party legal entity, and be able to disseminate information in a standardized message format, exchange information technology systems in the appropriate

language version, from EU registries to other competent registries of other states (Directive (EU) 2017/1132 of the European Parliament and of the Council...).

The above directive has a significant impact on human rights protection, as it provides for simplification of access to information, which especially allows for transparency (applies to consumers, investors and other stakeholders), pays attention to the protection of personal data (privacy and security of human rights) and ensures access to information for everyone (important for ensuring justice and equal opportunities for everyone).

All of the above cases have in common that the relevant company registers and, of course, business in general are always under the jurisdiction of the legislature and, accordingly, the state, and their organization is carried out through the relevant regulations. Subsequently, their organization is realized through the judicial and executive branches, depending on whether the relevant registration is carried out by specific courts or, possibly, by a special administrative body. The direct data entered into the registry and made available (public) to third parties ensured the security of both legal and business transactions. Thus, the information in the registers was considered to be true until proven otherwise, and the registers themselves were so-called public books. Thus, the state is interested in legal regulation of this sphere, in the implementation of practical application of legal norms and is successfully supported by it (Унапређен сервис "еРегистрација оснивања привредног друштва"...). With the creation of an electronic database (modern registers of business entities), the age of digitalization and the use of modern technologies at the stage of establishing a business entity, namely its registration, has begun. It is important to note that since the beginning of the twenty-first century, this trend has spread globally in the international arena. For example, in the Republic of Serbia, starting in the second half of 2018, it became possible to carry out the entire process of registering business entities online, without physically sending certain documents by mail, and the registration itself turned into a full electronic registration. Of course, in order for electronic registration to be possible, certain conditions must be met (the applicant must have a qualified electronic signature certificate, have the appropriate program installed on the computer, have a payment card with which to make payments, etc.)

However, this important step in providing electronic registration confirms previous statements that digital technology has made business easier for businesses, saved time and money, and has also uncovered many problems that did not exist before or that are existing dilemmas.

After the establishment of the Enterprise Registration Agency in Serbia, one of the dilemmas that still exists is whether the relevant administrative body, funded by the

non-governmental sector, can be even more professional and independent in its content than the direct judicial registry - the special registration department of the courts. At the same time, after the establishment of the Agency, the registration of business entities acquires the status of a legal entity, and this action has become a formal procedure that determines the will of the founder and registrar. That is, the entry of a business entity in this register is not declarative, but constitutive, when such an entity is new, different from the previous one, or the founders have changed. The continuing establishment of the Enterprise Registration Agency is appropriate and important. As I have noted above, the fact that the Agency is professional and independent will greatly simplify the acquisition of legal entity status by business entities. But I also believe that the procedure has become very simple. This means that obtaining the status of a legal entity through the Business Registration Agency requires legislative regulation, namely, a relevant law with a clearly defined procedure for obtaining the status, obtaining permits, entering into electronic databases, and submitting the necessary documents for registration. This will further ensure and further guarantee the digital protection of entities' rights.

The above allows me to understand that registration processes are quite significant for the protection of human rights, as they can quickly identify a digital enterprise and respond promptly in case of human rights violations, and allow the state and state bodies to control the activities of digital enterprises (where the most vulnerable are consumer rights, intellectual property rights, etc.). The process of acquiring the right to engage in digital entrepreneurship requires clear regulations and compliance with the relevant rights and obligations. However, it is worth noting that an improved system of business registration exists in the EU countries and is based on the Directive on the establishment of a central register of companies throughout the EU. And the specifics of digital rights protection are that today the only international legal document that regulates the processes of digital human rights protection and establishes sanctions for their violation is the GDPR. However, not all countries in the world are EU members and comply with the GDPR. Therefore, it is important for all countries of the world that are actively engaged in digital interaction to create an appropriate regulatory act on the protection of digital rights of individuals at the national level and establish clear regulations, procedures for the establishment and registration of business entities. Digital enterprises also have access to government services and programs, which standardizes the opportunities for all participants in the digital space, as everyone has the right to engage in this type of activity.

PART II

2.1. Study of human rights protection mechanisms in digital enterprises

2.1.1. Content monitoring mechanisms implemented by digital enterprises as one of the elements of human rights protection

Nowadays, the implementation of privacy and security of personal data by digital enterprises is important and quite relevant, since digital enterprises are a kind of database that stores significant amounts of user information, such as full name, address, phone number, user's email, personal correspondence, etc. It should be noted that even the most insignificant information about a consumer is important, as it can be used by fraudsters as a manipulative tool.

Therefore, data protection is important not only for business owners and consumers, but also for most countries that aim to ensure human rights for trust in the digital sphere and reduce the risk of legal problems.

Considering the EU regulatory framework for the protection of personal data of consumers, the following laws can be noted, namely:

1) General regulation on data protection, which provides rules for digital enterprises that collect, use and store personal data of consumers in their activities (EU GDPR..);

2) the Directive on electronic commerce, which sets out the rules on how businesses should collect and use personal information of consumers in their activities (Directive 2002/58/EC of the European Parliament and of the Council…);

3) the Directive on Privacy and Electronic Communications, which sets out the rules for how digital businesses should collect and use consumer personal information in electronic communications (Directive 2000/31/EC of the European Parliament and of the Council…).

The above laws have become the standard of privacy and security - not only from the point of view of the state and relevant companies, but also in the eyes of consumers, users and society as a whole (EU GDPR…);

Customers want their personal data online to be as secure as possible, but at the same time they expect innovative services, both online and in stores.

It is also well known that personalized products and services provide a strategic advantage. However, all personalization relies on one fundamental resource: personal data, without which it is impossible to personalize an individual.

Of course, personalization is a complex topic that can encompass several different levels:

1) In the simplest terms, personalization is based on known factors such as location based on IP address. Stores already use this feature, for instance, to display information in the local language and currency, but there are websites that go further by adapting content to the current situation in a particular location (such as weather or special events). Of course, even a free VPN program can thwart these efforts, but that doesn't change the fact that the practice is generally beneficial to companies.

2) On the other hand, people usually start using personal data when a user creates an account and becomes a regular customer. In this case, people have their basic data (name and surname, location, etc.), as well as their activity history. At this stage, most organizations start using the collected personal data for specific purposes, such as recommendation systems, personalized newsletters, and advertising.

3) The next level is advanced automation. In advertising or social media, companies have learned to use data as much as possible and wherever they can. And it is at this level that the greatest resistance is usually encountered, and personal data controllers face all sorts of problematic issues (Personenbezogene Daten – Wichtige Regelungen im Datenschutz…).

Considering privacy and personalization from the customer's point of view, the answer is simple: the user is ready to provide some personal data, but expects it to be used on his terms, and consent to its processing will be as easy to withdraw as to provide. Now, while expressing consent to personal data processing is something standard, the rules for withdrawing consent are not very transparent in practice.

Companies that would not have invested in advanced business technologies ten years ago are now doing everything they can online. Even if the company itself operates only stationary. A store or cafe wants to have its own special app. However, in many cases, it doesn't allow placing orders online and doesn't cover other typical online services.

Such apps are just a special way of collecting data. They allow consumers to participate in loyalty programs, receive personalized offers, and are encouraged to make further purchases.

Companies should ensure that personal data is clearly identified at the time of collection. At the same time, they should avoid situations where a specific individual can be identified with an appropriate amount of anonymous data. Most businesses and organizations appoint a data protection officer to manage data and ensure compliance with the principles of

personal data processing, including ensuring that customers' rights, including the right to be forgotten, are exercised.

The protection of personal data and privacy will no longer be limited to purely digital and commercial activities. For example, hyper-personalization will also appear in advertising on digital channels, blurring the line between virtual and physical reality, so data will be used both offline and online.

However, it is worth considering that in the case of advertising on digital channels, we are dealing with "banner blindness," which also makes personalization a phenomenon. According to statistics, the level of user distrust depends on the channel or device used. According to a 2019-2022 US report the highest level of distrust is in VR and AR (95%), and the lowest is in smartphones (81%), although this particular study did not include websites. It is logical that the same pattern applies to data processing consents (The Essentials for Successful Digital Transformation (DX)…).

We also have to understand that any new technology raises doubts and suspicions in the technological world, especially when it comes to maintaining personal data protection, so it takes the efforts of the first users to normalize this process (Yogesh K. Dwivedi , Elvira Ismagilova, D. Laurie Hughes…).

One of the biggest benefits of stricter data controls is that it allows for audience selection, eliminating people who subscribe to a newsletter, follow a company on social media, or perhaps even make one purchase but end up silently discontinuing services.

If a customer decides to register or provide their data, it means that they either want it or do not object to it. As a rule, their decision to provide personal data is directly related to the benefits they receive in return.

Another effect of the GDPR is to increase the responsibility of companies for the technological tools they use to an increasing extent. Companies now have to specify in their privacy policies which tools collect consumer data and confirm that the companies that create these tools have the appropriate permissions and consents to process the data. This also applies to cloud-based technology solutions, in which case the data should be stored in the relevant countries or regions. Fortunately, most cloud providers know how to protect data and comply with regulations, often better than many companies and governments. Since it is the proper protection of personal data that will ensure not only full protection of human rights, personal information and positive cooperation, but also help to avoid future mistakes and unpleasant situations.

The easiest solution - at least for large enterprises - is to use your own tools as much as possible. Not only does this eliminate external threats, but it also closes the data flow and has a reassuring effect on customers.

When we talk about data privacy, we naturally mean data related to specific customers and users. When the data is public and does not relate to specific individuals, it does not pose a threat of a breach. While e-commerce is not the only market for such data, it certainly has the most potential. For example, I can measure activity based on geolocated data, such as weather. I also have a wide range of Open Source Intelligence (OSINT) databases at my disposal (Ritu Gill What is Open-Source Intelligence…).

In this case, I am essentially combining known information with anonymous data and thus obtaining true market knowledge. And, for instance, if I have users who create accounts and give me more access to information, additional opportunities open up for me. Burger King used to use geolocation for rather controversial purposes, for example, to advertise food orders from home on rainy days. Therefore, on the one hand, this company can be said to have partially violated the personal data of consumers, and on the other hand, it was expanding the boundaries of its cooperation. People will undoubtedly remain concerned about the privacy of personal information. It's safe to assume that the pressure to comply with regulations will increase. Therefore, the first thing that the vast majority of companies should do is to improve data management - from ensuring security and access to data to ensuring full compliance with user privacy rules.

It is important to note that a digital enterprise actively monitors content on news portals as part of its digital marketing efforts. Sometimes such moderation leads to an escalation of tension, during which the norms of etiquette and morality are violated, but on the other hand, it leads to an increase in the discussion of certain issues. The monitoring of news content itself can be used in the future to promote the content on social networks, and the moderation of user discussions will help to avoid violations and identify possible problems.

As we can note, digital companies are using quite creative ways to use personal data to advertise their activities. Therefore, it is advisable for companies to develop appropriate strategies to encourage customers to willingly provide their data. Loyalty programs and other digital motivational tools are a perfectly balanced solution here, as they provide benefits for both the customer and the company. In my opinion, it would be logical to build a system of personal data protection for companies that advertise via the Internet or applications on the phone, including geolocation. Moreover, in today's environment, the implementation of privacy and security of consumers' personal data by digital enterprises is important and quite

relevant, since digital enterprises are a kind of database that stores significant amounts of user information, such as full name, address, telephone number, user's email, personal correspondence, etc.

2.1.2. Implementation of human rights protection in digital enterprises by European legislation

The international human rights protection system includes a core principle that is reflected in effective legal protection and the application of appropriate access to remedies when human rights are violated or significantly harmed. The purpose of reparation is primarily to ensure that such harm does not recur and to remedy and prevent any future harm to human rights.

It should be noted that legislative, public and, accordingly, financial scrutiny of specific corporate actions on human rights is steadily growing and improving. The next step is to consider remediation in line with the UN Principles, which are guiding, as companies are rapidly investing in due diligence of their supply chains, staff training, risk mapping, and of course suppliers, to further reduce human rights abuses.

For example, the UN Guiding Principles on Business and Human Rights emphasize and recognise reparation, namely: the duty of the state to investigate and punish and ensure the protection of human rights of violators (art. 1); the obligation of corporations to cooperate in matters of reparation, to provide reparation if they have caused or contributed to harm (Article 22).

In general, these UN Principles play a key role in facilitating access to redress.

For example, Article 30 of the UNGPs emphasizes that joint, multilateral and industry initiatives based on compliance with relevant standards have ensured that effective grievance mechanisms are in place. Such systems and standards for sustainable development are a type of multilateral initiatives (UN Guiding Principles on Business and Human Rights...).

When the rights of rights holders have been violated, there are reasons why they turn to the independent system of multilateral initiatives:

- accessibility (characterized by ease of navigation through the complaint procedure);

- trust and safety (due to the possibility of retaliation, it is easier to file a complaint with a third party than with the employer);

- the reality of the existence and operation of global supply chains. Thus, it is difficult to determine who is responsible for a violation in a transnational supply chain that is complex

and opaque. In some cases, it may be easier to lodge a complaint with a credible and reliable presence through an independent scheme.

Sustainable development systems can play a key role in remedying human rights violations and abuses, and can help to increase access to appropriate remedies. This is achieved through appropriate schemes of their own grievance mechanism, primarily for certified organizations. In this case, it is not only the existence of such mechanisms that is critical, but their effectiveness.

Effective grievance mechanisms in UNGPs have a clear understanding of what makes an effective grievance system, and ISEAL's work focuses on improving the capacity of community members to meet these criteria, referring to the relevant UNGPs accountability and remedy guidelines. Accessibility, for example, is a key aspect, and the grievance mechanism in principle allows rights holders to file complaints in different languages. Therefore, immediate legitimacy requires that the mechanism enjoys the trust of those for whom it is so difficult to invest in schemes to build dialogue, trust with relevant stakeholders, and to maintain legitimacy through their independence. To ensure that the aggrieved party has reasonable access to a source of information, expertise and advice, a focus on fairness is necessary to participate in the grievance process in an informed, fair and respectful manner.

Sustainable development schemes are used to improve the system, procedures and policies for recovery. The ISEAL Self-Assessment Tool for an Effective Grievance Redress Mechanism is a very important first step in helping community members to improve themselves.

Sustainability in promoting remediation at the local level and gaining knowledge about how best they can. Finding the right partners at the local level to support remediation and encouraging schemes operating to cooperate in the same region and sector are specific ideas that have emerged and are relevant today.

The human rights space itself, and of course business, is constantly evolving, as corporate responsibility for human rights is significantly regulated by legislative measures and sustainability frameworks are also in the spotlight. Along with recognising in those standards that address these rights, the role of the framework in remediation is fully traced. For example, this next step will be a key distinction between those who do not cause harm and those who seek to promote respect for and protect rights in business.

Council of Europe member states have an obligation to ensure to everyone within their territory the rights and fundamental freedoms enshrined in the European Convention on Human Rights (ECHR). This obligation also extends to the use of the Internet. Other

conventions and instruments of the Council of Europe related to the protection of the right to freedom of expression, access to information, the right to freedom of assembly, protection against cybercrime, as well as the right to privacy and protection of personal data are also applicable (Recommendation CM/Rec(2014)6 of the Committee of Ministers...).

States' responsibilities to promote, respect and protect rights include oversight of private sector companies. Human rights are non-negotiable and universal in nature, taking precedence over general conditions and standards imposed by the private sector.

The Internet is of general public value. Individuals, private entities, governments or communities rely on the Internet for their activities and have a legitimate expectation of access to its services that are non-discriminatory, affordable, accessible, sustainable, reliable and secure. Thus, no one should be subjected to unlawful, unnecessary and disproportionate interference with the exercise of their rights when using the Internet.

For the effective exercise of rights, users should be provided with appropriate support to understand their existing rights in the event of restrictions or interference with their freedoms and rights. Such support should include advice on how to access effective remedies. Given the opportunities that the Internet provides for accountability and transparency in the conduct of public affairs, users should use the Internet for their democratic lives.

In order to ensure the equal application of human rights and freedoms both online and offline, the Committee of Ministers, on the basis of Article 15.b of the Charter of the Council of Europe, recommends that EU Member States: review and evaluate on a regular basis, and, if necessary, repeal restrictions on the use of the rights under study on the Internet. It is believed that any restriction must be consistent with the achievement of a legitimate aim and its proportionality, especially if it is not in line with the ECHR case law; provide Internet users with access to reliable and effective legal protection if their rights are violated, which will significantly strengthen the issue of cordoning and cooperation between institutions. Depending on national regulations, this may also include a mechanism and process for redress by data protection authorities, court procedures, and ombudsmen; within and outside the Council of Europe, facilitate cooperation between non-state and state actors on legal procedures and standards; encourage the private sector to fulfill its corporate social responsibility; encourage society at large to use and legally disseminate the Guidelines.

The Annex to the Guidelines explains not only the remedies and access to them, but also enables users to know their rights and possible restrictions, with the Convention on Human Rights as a fundamental basis, which all EU Member States must implement.

In a modern democracy, access to the Internet is one of the most important means of exercising one's rights. That is, against a person's will, he or she cannot be disconnected from the network, except when it is done by a court order. It is important to note that this can also be used under specific contractual relations aimed at terminating the provision of services.

In general, access to the Internet should provide users with the opportunity to implement content, network services and applications, i.e. the network should be accessible and non-discriminatory. At the same time, public authorities should take all measures to facilitate access to the Internet, taking into account certain segments of the population with low income, disabilities or special needs, or those located in geographically remote areas. The user must also not be discriminated against on the basis of gender, skin color, language or religion, etc.

It is important to note that the right to search for, disseminate and generally receive information of one's choice means: to have access to information, express themselves online, freedom of expression (views on religion, political speech, etc.); expression may be restricted if there are signs of incitement to discrimination and violence. Restrictions must be legitimate, protecting order and national security, public morality, etc. They must also be communicated to the user; create and distribute content in a free form, taking into account elements of copyright or intellectual property rights; ensure protection of views by public authorities; the provider of the Internet and the relevant content bear corporate responsibility. In the case of inappropriate content policies, content may be restricted. These are important things to keep in mind for further decision-making.

In turn, the user has the right to: assemble and associate for peaceful purposes; freely choose a website or service; freely use available online tools to discuss government policy; develop and sign petitions.

The rights of the individual user related to the protection of rights and inviolability include: protection of personal data; secrecy of communication; secrecy of correspondence. Therefore, a person should be aware that his or her personal data is regularly processed, and that government agencies follow special procedures when processing it, subject to the user's consent and in accordance with the provisions of legislative acts. Also, the user should be aware that the processed personal data is transferred to third parties, but they can control their data: delete, store it, etc.

Confidentiality issues are also observed in work processes. Thus, the employer must notify the employee if he or she is being monitored or monitored in private correspondence or communication via the Internet in general.

In case of violation of any of the above rights, the user may request protection of his or her personal data.

It is important to constantly warn the user that the content a person publishes on the Internet will be available worldwide and may pose a real or future threat to his or her honor or dignity, security and confidentiality. Thus, if necessary, a person may request the deletion of information about him or her, which is carried out within the reasonable time limits established by law.

If necessary, a person may use effective legal remedies, such as investigation, apology, explanation, restoration, response, compensation, etc.In this case, the Internet service provider should provide all information and support in data protection and minor violations. In the case of full-fledged criminal activity, the relevant law enforcement authorities should protect against violations such as fraudulent manipulation, forgery, interference or illegal access and take appropriate measures, such as sanctions.

In the course of determining and defending an existing Internet-related charge, a user is entitled to: within a reasonable time, to a fair, impartial trial; after exhausting all available national remedies, to apply to the ECHR. These aspects are important because they provide for fundamental rights in the digital sphere, in order to reduce negative consequences in the future. It can also be noted that European legislation quite successfully regulates all possible rights of individuals in the digital sphere to ensure the proper exercise of the right to freedom of thought, privacy (protection of personal information in the digital sphere), the right to accessibility (access to information), the right to form and join any associations, the right to normal treatment of everyone regardless of their race, gender, sexual orientation, religious preferences, etc. Thus, if a person properly exercises his or her rights in the digital space, there is a clear and comprehensive system of European protection. In my opinion, the mentioned above do not require any additional legal regulations at the moment.

PART III

3.1. Implementation of sanctions and other types of liability for digital enterprises

3.1.1. Establishment of administrative and financial sanctions for digital enterprises in case of human rights violations

In the system of legal liability, administrative and financial sanctions applied to digital enterprises in case of human rights violations have a number of features and relevance, as they ensure the rules of substantive and procedural law, the repressive nature of financial sanctions and administrative fines, which are important elements in the system of protection of human rights and freedoms.

Over the past decade, European legislation has undergone significant changes in the system of sanctions, namely, there has been a significant progression of coercive measures in the form of financial penalties and administrative fines, which are listed in 200 provisions. At the same time, criminal sanctions were automatically concealed, and the omission of guarantees of the criminal procedure, which is not a positive consequence for the digitalization system and the protection of human rights in it (The Essentials for Successful Digital Transformation…).

At the same time, it is important to consider legislative shortcomings that are reflected in the regulation of the general principles of imposing financial penalties and administrative fines, and which in general lead to a dangerous situation from the point of view of protecting human rights and freedoms. Establishing clear substantive and procedural rules in proceedings for the imposition of financial penalties and administrative fines would serve to implement the principles of a democratic state governed by the rule of law, as well as the principle of equality before the law. The current legal situation leads to unequal treatment of subjects of administrative and financial liability who are subject to punishment on different legal grounds. In order to properly define the requirements for substantive and procedural principles used in imposing sanctions, it is necessary to define this legal instrument and determine its goals and functions.

The Common Foreign and Security Policy (hereinafter referred to as the CFSP) currently has a great potential for Europe's strategic autonomy. Thus, since the entry into force of the Treaty on European Union (hereinafter referred to as the TEU) on November 7, 1993, the CFSP has been institutionalized in the basic law in Title V, Chapter 2, Articles 21-46. According to the content of the TEU, through "restrictive measures (sanctions)" the

CFSP has an operational toolkit that is increasingly used to achieve the foreign and security policy objectives set out in Article 21 of the CFSP. Among these goals is the preservation and strengthening of the rules-based multilateral approach as the basis for world peace and international security (Treaty on European Union (TEU) / Maastricht Treaty…). In my opinion, digital rights are a matter of common foreign and security policy, as digital rights are closely related to personal data protection and are an integral part of everyone's security.

The use of administrative and financial sanctions by the EU is partly based on relevant UN Security Council resolutions. However, as the permanent members of the UN Security Council have become less and less likely to agree on multilateral UN sanctions over the past 20 years, the number of autonomous EU sanctions without an international mandate has increased. The growing importance of the EU's autonomous sanctions is reflected in their respective strategic documents, in particular on:

- European and global security (2003, 2016);
- cyber security (2013, 2017);
- maritime security (2014, 2018),

as well as in the Human Rights and Democracy Action Plan for 2020-2024.

In addition, some national strategy documents of member states describe this tool of the CFSP as a precautionary measure in crisis and conflict prevention. Sanctions can also be useful in stabilizing and promoting peace by helping to isolate perpetrators and support constructive forces alongside other measures such as mediation (Common Foreign and Security Policy).

The EU sees itself as a community of laws in its external activities. As such, it always seeks to impose autonomous sanctions in a manner that is consistent with fundamental rights and legally based. The relevant legal requirements stem from both multilateral agreements and international treaties that have committed the EU to their observance.

In addition, the EU is obliged to comply with the Charter of Fundamental Rights of the European Union (EU Charter), which defines fundamental rights and principles that have the same legal force as European treaties in accordance with Article 6, paragraph 1 of the Treaty on the Functioning of the EU (Communication from the Commission to the European Parliament…).

Paragraph 3 of Article 52 of the EU's Treaty on Economic Cooperation also establishes that it is necessary to ensure the preservation of the principles of the rule of law set out in the European Convention for the Protection of Human Rights and Fundamental Freedoms of the

European Council (Consolidated version of the Treaty on the Functioning of the European Union…).

In general, the application of autonomous EU financial sanctions in accordance with Article 48 of the EU's Charter of Economic Relations (presumption of innocence and right to defense) cannot be equated with a legal conviction for previous crimes. This is an important administrative measure that does not involve punishment or confiscation, and therefore does not violate property rights. Nevertheless, a ban on the disposal and provision of property can have virtually the same effect as judicial confiscation or even confiscation of property (Consolidated version of the Treaty…).

For example, it can greatly affect civil debt relations. Therefore, academic and legal critics have charged that the consequences of the respective prohibitions for the persons concerned are very similar to those of "civil death". In addition, the prohibitions on disposition and granting constitute a violation of the freedom of capital (para. 1) and payments (para. 2) under Article 63 of the Treaty on the Functioning of the European Union, which in principle should be ensured both within the EU and between the EU and third countries (Communication from the Commission to the European Parliament…).

In this context, the principle of proportionality enshrined in Article 52(1)(2) of the Charter of Fundamental Rights of the European Union is important. According to this principle, the measures applied must be appropriate, necessary and adequate to achieve the foreign and security policy pursued in each case. The relevant decisions under the CFSP on the application of EU autonomous sanctions should be formulated in such a way as to achieve the fairest balance between the recognized violation and the relevant consequences. To this end, it is necessary to have clear lists of persons subject to sanctions, supported by adequate evidence, in accordance with Declaration 25 on Articles 75 and 215 of the Treaty on the Functioning of the European Union (hereinafter TFEU).

Therefore, the Council must base the lists of individuals and legal entities on reliable grounds, which must be substantiated by the link between the relevant actions constituting the violation, on the one hand, and the damage caused to foreign and security policy as provided for in Article 21 TFEU, on the other hand, in accordance with Article 296(2) TFEU (Consolidated version of the Treaty on the Functioning…). Such a link must be substantiated in accordance with Article 41 of the EU Charter of Fundamental Rights (right to good governance) so that possible excessive assumptions or allegations of reputational damage can withstand judicial scrutiny. In addition, a transparent and legally enforceable process should

be ensured to allow individuals and legal entities to defend their rights in the event of sanctions.

The key is the judicial review of the legality of the decisions of the CFSP in accordance with Article 47(2) of the EU Charter of Fundamental Rights (the right to an effective remedy and an impartial tribunal).

Although the CJEU does not normally have jurisdiction over the CFSP under Article 24(1) of the Treaty on European Union and Article 275(1) TFEU, the application of autonomous EU financial sanctions is included in the exceptions set out in Article 263(4) TFEU, which allows individual stakeholders to successfully challenge their inclusion in the sanctions lists by way of delisting. The above indicates that if it is possible to appeal the decision to impose financial sanctions, it is possible to apply to the EU court with the relevant list of appeals. In my opinion, this case is a certain gap in the legislation and needs to be improved by prohibiting the appeal of the decision in similar cases.

The case law on this issue shows that the authorization to cancel under Art. 263(4) TFEU has been significantly expanded after 2 decisions in the case: «Rosneft» in March 2017 («Rosneft» in March 2017 ECLI:EU:C:2017:236…) and «Bank Refah Kargaran» in October 2020 («Bank Refah Kargaran» In Case C134/19 P…). In these cases, the validity of the evidence submitted in relation to certain lists was considered. After the publication of these cases, the CFSP may also be reviewed by the EU Court of Justice through a preliminary ruling in accordance with Article 267 TFEU (Further erosion of the Polish democracy…).

Currently, third countries directly affected by the EU's autonomous financial sanctions can challenge the relevant legal bases through a repeal. Before a court of law, evidence of the alleged acts, such as embezzlement, weapons financing, terrorism, and human rights violations, must be supported by convincing evidence.

In some cases, such as cyber attacks, the identification of responsible persons is technically extremely difficult. In general, the reform of Article 105 of the EU Procedure Rules, which came into force in July 2016, facilitates the collection of evidence by allowing for expedited review of documents marked "not secret" in accordance with Article 6, paragraph 1 of the Agenda of the Council of the European Union. However, the legal review of the legality of the CFSP decisions does not include a substantive assessment of the relevance or legality of the grounds for individual lists. The assessment of their relevance remains a matter of a political decision of the Council.

Considering further the procedural rules for the implementation of administrative and financial measures, it would be advisable to expand the scope of the analysis and pay

attention to and study the practice of Poland as an EU member state and its implementation of personal data protection.

Personal data in Poland is of great importance as it plays an important role in many areas of life. Continuous technological advances mean that both private businesses and public institutions can easily manage and use it in various ways and for various purposes in their activities.

However, the problem was to ensure that the processing of such data was properly controlled. In order to meet the expectations of citizens, the EU authorities led to the adoption of a regulation on enhanced security standards that guarantees the right to privacy and data protection. The established law is uniform for all EU countries. This is a convenience created primarily for the citizens of the Community, who will be able to assert their rights in connection with data protection violations in a simplified manner.

At the same time, on May 25, 2018, Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as the "GDPR", came into force (Regulation (EU) 2016/679 of the European Parliament and of the Council…).

In order to adapt the GDPR to the Polish legal order, it was also necessary to prepare a new national law on personal data protection. The law entered into force on May 10, 2018 (Regulation (EU) 2016/679 of the European Parliament and of the Council…) and, in terms of its scope, complements the EU General Data Protection Regulation.

In the context of the changes resulting from Regulation 2016/679, attention should be paid, among other things, to the wording of the definition of "administrator". This term has replaced the previous definition (from the previous European regulation on personal data protection - Directive 95/46/EC) of "data controller".

Thus, while the legal acts limited the concept of a data controller, excluding the element of possible joint administration, according to the new legislation, a controller - administrator is a natural or legal person, state body, agency or other organization that determines the purposes and means of processing personal data not only independently but also jointly with others. Due to its responsibility and scope of powers, the administrator's function is key in the context of data protection.

However, according to representatives of the doctrine, the newly introduced regulatory decisions on the definition of an administrator have not eliminated the problem of assigning the status of an administrator. The introduced legal provisions on personal data protection

significantly expand the scope of obligations of entities that collect and use this data. In particular, attention should be paid to the obligation to appoint a data protection officer (Guidelines for data protection officers ("DPOs")…).

The tasks of the inspectors are regulated by Art. 39 R. 1 and Art. 38 R. 5 and 6 GDPR According to these rules, the inspectors are primarily responsible for informing the controller (administrator) and processor, as well as employees who process personal data, about their obligations under the GDPR, monitoring and complying with their regulations. Other responsibilities include, but are not limited to:

- reformulating provisions for obtaining consent to the processing of personal data;

- implementing appropriate data security procedures and measures, as well as reporting to the supervisory authority on any identified personal data protection violations (Justification of the government bill on the protection of personal…).

At the central level, a new supervisory authority responsible for personal data protection was also appointed - the President of the Personal Data Protection Authority, hereinafter referred to as the "President of the Personal Data Protection Authority". The rules for the appointment of this body, dismissal and term of office are regulated by Chapter 6 of the Law on Personal Data Protection (Ustawa z dnia 10 maja 2018 r. o ochronie…). Among the many powers granted to the President of the Personal Data Protection Authority, the power to impose administrative fines is particularly important in the context of the issues under discussion. According to the previously effective Law on Personal Data Protection, the only possible monetary sanction that the supervisory authority could impose on a data processor within its powers was a so-called compulsory fine in the amount determined in accordance with Article 121 of the Law on Enforcement Proceedings in Administration. Its maximum amount could not exceed PLN 10,000, and for legal entities and organizational units without legal personality, the amount could not exceed PLN 50,000.

However, the penalty was characterized by a low degree of effectiveness, as it could only be imposed if the entity did not comply with the provisions set out in the decision. The new law has changed the existing rules for imposing fines and set their amounts to an incomparably higher level. This is a deliberate action that somehow "mobilizes" both private companies and government agencies, which have so far been negligent in data processing, to better protect such sensitive information as personal data. This is primarily due to the right to privacy and information autonomy that every individual has. Sometimes, the only objectively possible way to ensure the fulfillment of the above guarantees is to impose high fines. This is mainly how EU Member States can force the recipients of the legal provisions of the

regulation to respect and comply with them. More lenient sanctions, including all types of warnings, are ineffective and only to a limited extent can prevent future violations.

Although the institution of an administrative fine has existed in the Polish legal system for many years, the legal definition of this concept was introduced only in 2017. Thus, Art. 189b of the Polish Code of Administrative Procedure states "expressis verbis", which means "administrative fine", which is characterized by a financial sanction defined in the law imposed by a public administration authority by way of a decision as a result of a violation of the law, consisting in the failure to fulfill an obligation or violation of a prohibition imposed on a natural person, legal entity or organizational unit without the status of a legal entity (Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania…).

The mentioned editorial subdivision is a part of Section IVa of the Code of Administrative Procedure of Poland (hereinafter referred to as the CAP), which establishes general principles for assessing and imposing administrative penalties (Act of April 7, 2017 amending the Act - Code of Administrative Procedure…).

Proceedings leading to the imposition of a fine in accordance with the provisions of the Law on Personal Data Protection and the GDPR are conducted in an administrative manner, so in this case the provisions of Section IVa of the Polish Code of Administrative Procedure will apply, as defined in Article 1, paragraphs 1 and 2 of the Code of Administrative Procedure (Uzasadnienie rządowego projektu ustawy…).

At the same time, in accordance with Art. 189a of the Polish Code of Administrative Procedure, the direct application of the standards included in this section may be limited due to the introduction of detailed regulation of legal proceedings provided for in Art. 189a § 2 of the Polish Code of Administrative Procedure (in accordance with the principle of lex specialis derogat legi generali) (Uzasadnienie rządowego projektu ustawy…).

Such a case occurs in accordance with the provisions of the Law on Personal Data Protection, as provided for by the conflict of laws provision expressed in Article 106 of the Law: "The provisions of Articles 189d-189f and 189k of the Law of June 14, 1960 - the Code of Administrative Procedure shall not apply. The admissibility of certain provisions of the Code of Administrative Procedure is disabled in order to enable the direct application of the GDPR provisions" (Ustawa z dnia 10 maja 2018 r. o ochronie danych).

Returning to the very concept of administrative penalty, attention should be paid to the semantic conditions associated with this concept. Repeatedly, financial sanctions, which are in fact also administrative fines, have been reflected in the following forms: increased fee,

penalty fee, additional amount, additional tax liability, and financial penalty (Żakiewicz-Zborska, K. «Dr Edyta Bielak-Jomaa: Attention…).

The current practice of different terminology has not contributed to compliance with the standards of correct legislation, therefore, to ensure clarity of the law and terminological consistency, financial penalties of an administrative nature, previously established in numerous acts of norms, should remain unchanged, and the new norms should be called "administrative fines".

A correlate of the concept of punishment is a sanction. It is believed that a sanction is one of the defining features of law and a guarantee of the effectiveness of a legal provision. The concept of a sanction, like the concept of a fine, is always associated with a certain discomfort for the addressee. In general, the institution of a fine is classified as one of the types of administrative penalties along with the sanction of enforcement. However, there are many other divisions in legal doctrine based on different criteria. For this reason, the division of sanctions is loose and not strongly methodological.

For example, based on the criterion of the responsible entity, sanctions are divided into defined and unspecified, monetary and non-monetary sanctions.

The division by the criterion of the responsible entity (individuals and legal entities, public authorities) divides sanctions into absolutely certain and absolutely indefinite sanctions (Staniszewska, L. (2017). Aligning administrative fines with democratic principles…).

However, in my opinion, this division should be further subdivided by the criterion of severity of sanctions into financial and non-monetary sanctions.

Non-monetary sanctions reflect the negative legal status of the violator, since the right to carry out activities is deprived. Financial sanctions also reflect the negative state of the violator, but are less severe because the administrative decision does not deprive the violator of the right, but imposes a fine in the form of a fixed amount of money (Błachucki, 2015).

Financial sanctions are currently the most effective means and ways to ensure the fulfillment of administrative and legal obligations.

With regard to administrative sanctions, it is worth noting Chapter 11 of the Law on Personal Data Protection. Thus, Articles 101 - 108 of the Law reflect the general conditions for imposing an administrative penalty (Act of May 10, 2018 on the protection of personal data…).

As already noted, in Poland, the authority authorized to impose this type of sanction is the head of the Office for Personal Data Protection, while in some EU countries (Denmark and Estonia), courts are vested with such powers.

In addition to the authority to impose fines, the Head of the Personal Data Protection Authority also uses legal powers. These are additional measures that are more lenient than administrative fines.

The supervisory authority may apply them both simultaneously with the imposition of a financial penalty and instead (if it considers that the use of a substitute in the form of human rights powers is sufficient to achieve the purpose of the penalty).

The types of such powers include:

- issuing warnings;

- issuing warnings or ordering to notify the data subject of a data protection violation. The full list of rights is contained in Article 58(2) GDPR.

Administrative fines can be imposed on both personal data controllers and entities that process data on their behalf. These can be both private individuals (including individuals and businesses) and public institutions.

The possibility of penalizing public organizations is contained in Article 83 R. 7 of the GDPR. The EU authorities have left the decision on the admissibility of punishing public institutions to the Member States, so Polish law has decided to introduce such a possibility.
The threat of imposing financial sanctions on public institutions is provided for in Art. 102 of the Law and includes:

- public authorities, public administration bodies, state control and state security bodies (in particular, the Sejm, the Senate, the Council of Ministers, the Supreme Court of Control, the Polish Financial Supervision Authority, the Police, the Military Police)

- universities;

- National Fund.

The catalog of sanctions specified in the regulation, although closed, may be expanded to include sanctions imposed by national lawmakers. This decision was mentioned in paragraph 149 of the introduction to the GDPR. This catalog of sanctions may include criminal penalties in addition to administrative fines. It is important to note that the imposition of criminal sanctions for violations of national regulations and the imposition of administrative sanctions should in no way lead to an increase in penalties. A topical issue that causes controversy among entities potentially facing fines centers on the amount of financial sanctions.

Thus, the financial sanctions threshold is divided according to the perpetrators of the offense - public and private entities. However, it should be assumed that, for simple reasons, there is a significant imbalance between the above entities in favor of public institutions. In particular, imposing high fines on public authorities and private entities will have little repressive effect, since the revenues received from administrative fines make up the total revenue of the State Treasury. Therefore, it would be extremely pointless to impose monstrously high fines on institutions that are fully financed from the state budget. In other words, the money would de facto go there anyway (Uzasadnienie rządowego projektu ustawy o ochronie…).

However, it is worth paying attention to some changes in the catalog of entities to which the lowest threshold of financial sanctions will apply - the National Bank of Poland, which is a state institution but self-financed.

Thus, a violation of one of the three main directives on the application of fines under the GDPR (i.e. the principle of proportionality) can be asserted in a situation where a fine of the same amount is imposed, for example, on the National Bank of Ukraine, Poland and the National Health Fund, whose activities are fully financed from the state budget.

The maximum amount of such a financial penalty that may be imposed on public institutions listed in Article 102 of the Personal Data Protection Act is PLN 100,000. The exceptions are public cultural institutions and local government institutions. Given the main purpose of their activities, namely the dissemination and creation of equal access to cultural goods (Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia…), it was decided to set the lowest fine - up to PLN 10,000.

The financial responsibility of non-governmental entities is at a much higher level. The Regulation specifies two fine thresholds. Their value is expressed in euros, so they need to be converted into Polish currency based on the average exchange rate published by the National Bank of Poland:

- Threshold 1: up to EUR 10,000,000, and in the case of an enterprise, up to 2% of its total annual global turnover for the previous financial year;

- Threshold 2: up to EUR 20,000,000, and in the case of an enterprise, up to 4% of its total annual global turnover for the previous financial year.

Penalties imposed on individuals who are not entrepreneurs are set at threshold amounts. However, financial penalties imposed on businesses are determined according to a percentage of revenue, which allows for an adequate fine to be imposed in direct proportion

to the revenue received. This solution makes it virtually impossible to estimate the maximum amount of a fine imposed on a company.

The financial penalty set out in threshold 1 is imposed pursuant to Article 83(4) GDPR for minor infringements, such as, for example, the failure of a personal data controller to register processing activities in accordance with Article 30 GDPR.

The grounds for imposing a fine set forth in threshold 2 relate to a more serious category of violations related to the basic principles of processing of ordinary and special category data, including the conditions for obtaining consent, as well as violations of other obligations listed in Article 83(5) GDPR and in certain provisions of the regulations defining these obligations. A higher threshold of liability also applies in the case of non-autonomous penalties, i.e. those sanctions imposed in case of failure to comply with orders referred to in Article 58(2) GDPR.

The supervisory authority decides on the imposition of an administrative penalty and, if there are grounds, the amount of the penalty based on the penalty orders set out in Article 83(2) of the GDPR. This provision defines 11 circumstances that are intended to help regulatory authorities determine an adequate and proportionate penalty, taking into account all the circumstances in a particular case.

These 11 circumstances are summarized in the following categories:

- elements related to the incident constituting the violation (nature, seriousness, duration of the violation, degree of responsibility);

- behavior of the controller (administrator, processor) in relation to the breach (current attitude to compliance with personal data protection standards);

- behavior of the controller (processor) after the breach (minimization of damage, method of notification of the breach, compliance with corrective measures);

- consequences of the breach (number of people affected and amount of damage).

The above circumstances should also include certain aggravating and mitigating factors that may have an impact in the context of a particular case, such as financial benefits received directly or indirectly in connection with the violation or avoidance of losses.

In addition to the circumstances specified in the GDPR, when applying both administrative fines and financial sanctions, it is important to comply with the principle of proportionality, which is reflected in Article 5 R. 4 of the Treaty on European Union. Along with this, EU law, in the provisions of Recital 151 of the GDPR, states that sanctions must not only be proportionate, but also effective and dissuasive.

The procedural structure for imposing an administrative fine is as follows. The Head of the Department of Personal Data Protection issues an administrative decision, which may be challenged by filing an appeal against the said decision. Pursuant to Article 105 of the Law on Personal Data Protection, an administrative penalty is imposed 14 days after the expiration of the term in case of filing an appeal (complaint) to the administrative court, and 14 days after the administrative court decision enters into force in case of imposing a penalty (Wyrok NSA z dnia 10 marca 2010, sygn. I FSK…).

Analyzing the Polish CAP, it is worth noting that in the part of the collection of fines and limitation periods, general rules are used, in accordance with Articles 189g, 189h, 189i, 189j. Along with this, Art. 189 defines the issue of mitigation of the application of a certain penalty (Wyrok NSA z dnia 2 marca 2016, sygn. II FSK 2474/15…).

At the same time, it should be noted that there are cases when the President of the Office of Personal Data Protection, at the request of the fined person, postpones the payment of the fine or divides it into appropriate parts. After that, the relevant public administration authority, within its discretionary powers, decides on the expediency and justification of the said request (Wyrok NSA z dnia 2 marca 2016, sygn. II FSK 2474/15…).

It is worth noting that this issue is resolved taking into account objective circumstances, special reasons indicated by the fined person, including emergencies, and the financial situation of the latter.

In addition, when an administrative fine is imposed and is to be paid in installments, the interest is accrued for each installment separately.

Along with this, the law defines the right of a fined business entity to apply for exemption from paying an administrative fine (Wyrok NSA z dnia 2 marca 2016, sygn. II FSK 2474/15…). The above allows me to understand that the practice in the analyzed area means that the provisions I have mentioned are mainly theoretical in nature and they are advantageous to national legislation. In my opinion, there is no need to improve the situation at the moment.

So far, there have been several cases of fines imposed in the European Union in connection with the implementation of the GDPR. The violations concerned access to the patient medical data management system. The audit found that the number of registered accounts with access to patient medical data was more than three times the number of doctors working at the hospital. The hospital was fined a total of €400,000 for failing to exercise due diligence in data processing and breaching authentication methods (Uzasadnienie rządowego projektu ustawy…).

It is currently difficult to determine whether the ambitions of the EU authorities in adopting the new General Data Protection Regulation (GDPR) have been realized. However, there is no doubt that paying a high fine effectively influences the imagination of entities that could potentially be subject to sanctions and thus makes them comply with the law. The first cases of financial sanctions show that the newly adopted regulations are not just dead rules, but effective tools that guarantee the security of personal data protection. Thus, I can observe that the above is not only a theoretical aspect, but is also actively applied and implemented in practice.

In my opinion, if a sufficient level of protection of confidential information, such as our personal data, can be ensured only by introducing and imposing high fines, then such a measure should be fully supported. However, it is important to note that these sanctions are important not only in relation to personal data protection, but also in relation to the protection of digital human rights in general.

When applying administrative and financial sanctions, the relevant regulatory authorities strictly adhere to the principles of a democratic state governed by the rule of law, equality before the law, proportionality, efficiency and consistency. The main types of sanctions studied include: increased or penalty payment, additional charge of the amount, additional charge of tax liability, financial sanction, and non-monetary sanctions. When applying sanctions, the governing body is guided by the criterion of the certainty of the offender, for example, if the offender is an individual as a business entity, the minimum penalty will be applied, and in the case of a state body, the maximum penalty will be applied. The peculiarities of sanctions are that the imposed sanction can be appealed or the required amount can be divided into separate payments, the interest for which is charged separately (Fedorenko, 2022, p. 83). From my point of view, this is the tool that will help to avoid violations of not only general but also digital human rights as much as possible.

3.2.1. Determining the types of legal liability for digital enterprises that violate human rights on a regular basis

Today's realities force digital enterprises to increase the level of sustainable yet flexible growth of companies' competitiveness by developing and transforming their digital landscape (starting with raw materials), (By James Sullivan and Fawn Fitter How to make sustainable) and the main supply chain to quickly meet the changing needs of customers (The Essentials

for Successful Digital Transformation…) with more personalized service and order fulfillment, modernization and implementation of innovative traditional business models.
Since it was the COVID-19 pandemic that forced digital businesses to get rid of outdated systems and digitalize and modernize their work processes, it is worth noting a McKinsey survey that showed that after the pandemic, many respondents admit that their companies' business models are outdated, 11% of respondents believe that current business models will remain economically viable until 2024, and 64% say that their companies need to build a digital business in order not to disappear (The new digital edge: Rethinking strategy…).

This suggests that the new processes of digitalization and modernization of work processes will also lead to the emergence of various new types of liability for human rights violations in business.

In general, the concept of responsibility is used in various scientific fields: law, philosophy, sociology, psychology, ethics and other areas of knowledge. However, the essence of responsibility is the same regardless of the area of its existence.

Legal liability is one of the most important guarantees of observance of human and civil rights and freedoms, which solves the main tasks of ensuring social stability, protecting society from criminal attacks, strengthening and protecting the state (Fedorenko, 2022. p. 82).

Thus, the concept of responsibility is generally considered to be a multidimensional aspect; it has a philosophical and methodological character, conveys a special social and moral attitude of an individual to society as a whole, and the fulfillment of his or her moral and legal duty.

At the same time, however, responsibility in different branches of law is highly specific. In the context of the development of the information society, new challenges and threats are constantly emerging, and the issues of legal liability are of particular importance.
Considering in more detail the existing legal liability of digital enterprises, it is necessary to take into account that their liability depends on the type of claim made by the end user.

When establishing and implementing joint and several liability, it is important that the online store that received the complaint had an excellent contractual relationship with its supplier, and in the event of a complaint about the product for this reason, the latter agreed to assume responsibility through the technical support service and refund the costs incurred by the user (refund the amount paid), (Alexi, 2008, p. 177).

The peculiarities of joint and several liability also include the fact that if a certain product defect appears within the first 6 months, it is considered to exist at the time of delivery of the goods, so in theory, an online store has the right to demand that the consumer

prove that the defect existed at the time of delivery of the goods to the latter. If the online store purchases its products from a supplier that does not have a company or permanent establishment in the European Union, the supplier is liable instead of the manufacturer. If the products caused damage to the consumer, only the manufacturer is held liable. In my opinion, in order to avoid problematic issues with the consumer, namely, the issues of establishing who will be liable for the damage caused, it is important for digital businesses, such as online stores, to determine their intermediation in this case in order to preserve their reputation. In other words, the latter inform the user (consumer) about their role as an intermediary in the transaction and ensure that the professional providing the services has the appropriate licenses and permits to operate.

Analyzing further and exploring digital liability for human rights violations, it is worth mentioning that it covers such important aspects as respect, confidentiality, responsible participation, and more. The above suggests that the rights of digital users include obligations and digital laws that must be observed. In general, the business sector aims to regulate and level the playing field for all digital companies, regardless of their size, guided by two important legal acts: the Digital Markets Act and the Digital Services Act (Digital Markets Act and the Digital Services Act…).

When looking at the first law on digital markets, it is important to note that at its core it seeks to promote innovation, development and competitiveness, while helping smaller or newly established companies to compete with larger ones. The main goal of this law is to eradicate unlawful actions against companies and consumers.

The Law on Digital Services focuses on creating a safer digital environment for users and digital businesses by protecting fundamental rights on the Internet. The problems addressed by this law include, in particular, the trade and exchange of illegal goods, services and content on the Internet, and algorithmic systems that increase the spread of disinformation.

The above indicates that digital marketing (enterprises) must know and unquestioningly comply with the laws that directly affect it, as non-compliance will lead to appropriate (financial) sanctions.

When exploring the concepts of a common digital system, service and digital content, it is important to note the provisions of European Directive 2019/771 of May 20, 2019 (L'idée de créer un droit européen des contrats remonte à 2001…), which reveals certain aspects of contracts for the sale of goods. Thus, according to this, a digital system is defined as a set of interacting elements that combine digital content or a digital service, are interconnected with

such content or service, and the absence of such content or service will prevent the system from properly performing its direct functions (L'idée de créer un droit européen des contrats remonte à 2001…).

Digital content itself includes data created and provided in digital form (L'idée de créer un droit européen des contrats remonte à 2001…). A digital service corresponds to a service that allows a consumer to create, process, store or share or access data in digital form or a service that allows the exchange of data uploaded or created by the consumer or other users of that service (L'idée de créer un droit européen des contrats remonte à 2001…).

Exploring liability at the European level further, it is important to note that numerous directives affect the law of obligations on a contractual basis (e.g., consumer protection) or on a non-contractual basis (e.g., defective products). But to date, despite attempts at European harmonization, there is no unified European contract law (Cf. 2.1.1 pour la définition du contrat…).

Therefore, in my opinion, it is advisable to examine the legislation of one of the most developed countries of the European Union, namely France, on the mechanisms for protecting rights in agreements or contracts. For example, Art. 1170 of the French Civil Code states that any provision that deprives the debtor's essential obligation of its essence is considered unwritten (Cet article 1171 est issu de la réforme…). Thus, this rule of law aims to ensure that the contractual arrangement corresponds to the obligation promised by the supplier. This includes provisions limiting liability under which the debtor has little incentive to fulfill a substantial obligation to the creditor. For example, a hosting contract should reflect a significant limitation of penalties in case of non-compliance with the quality of service (Cet article 1171 est issu de la réforme…).

Art. 1171 of the same code guarantees that any non-negotiable provision determined in advance by one of the parties that creates a significant imbalance between the rights and obligations of the parties to the contract shall be deemed unwritten (Cet article 1171 est issu de la réforme…). Undoubtedly, this article covers: provisions on limitation or exclusion of liability; provisions excluding legal guarantees; provisions limiting the member's right to act; provisions on competence; provisions on reconciliation, reduction of limitation periods, etc.

Considering the French Consumer Code, it is worth noting that its provisions primarily protect the consumer and define this category of persons as a "weak party" in contractual relations.

An important tool for consumer protection is the concept of an unfair clause in Article L212-1 of the Consumer Code, which states that in contracts, clauses whose purpose or effect

is to create a significant imbalance to the detriment of the consumer are unfair between the rights and obligations of the parties to the contract (Article R212-1 pour les clauses abusives de manière…).

To summarize, it is important to note that a consumer association can act and has the ability to consolidate a series of minor losses taken separately and not offer impunity to an unscrupulous supplier and act in the interests of the collective on a collective basis: Art. L621-1 of the Consumer Code "...to exercise the rights recognized by a civil party to a case regarding facts that cause direct or indirect harm to the collective interests of consumers"; Art. L621-9 - by joining forces with the consumer, they can also claim compensation for material damage caused to consumers by filing a class action lawsuit (Article R212-1 pour les clauses abusives de manière...).

Considering trade law, it is important to note that for relations between professionals, the concept of restrictive competition in the French Commercial Code plays a role similar to that of the concept of unfair position in the Consumer Code, as it provides for the restoration of the contractual balance in commercial relations (L'ancien article L442-6-I du Code de Commerce…).

Thus, according to Article L442-1-I of the Commercial Code, among the restrictive acts of competition is the fact of "subordination or attempts to subordinate another party to obligations that create a significant imbalance in the rights and obligations of the parties". Art. L442-4-I of the Commercial Code allows the Minister of Economy to intervene in the process and impose sanctions on actions that restrict competition (Article 1240 (anciennement 1382) du Code civil…).

It is important to note that the general principle of civil liability is liability for fault and contractual liability (Article 1240 (anciennement 1382) du Code civil…). In my opinion, the example of France applies the most successful means of protection against digital human rights violations.

In civil law when analyzing contractual liability (Fedorenko, 2022. p. 85), it is important to note that it applies when losses were caused by improper performance of a contract that obliges the debtor (supplier) and its creditor (customer) to compensate for damage. Such contractual liability involves a combination of three elements: breach of contract (failure to fulfill contractual obligations), damages, and a causal link between them. If the said breach of contract results in direct damage to the creditor, the latter must prove the debtor's fault and the causal link between the breach of contract and the damage in order to hold its debtor liable and receive compensation for its damage.

Thus, the creditor must prove that the improper performance of the contract is due to the debtor's failure to act with all due care. In a performance obligation, the mere fact that the expected result is not achieved indicates the debtor's failure, as it would normally have been diligent to achieve the result it undertook to achieve. In practice, proving the debtor's fault is often confused with proving poor performance. In this case, the debtor must be relieved of this fault by proving that the improper performance was the result of force majeure. In an online services agreement, the agreed obligation may, of course, be affected by non-performance, improper or untimely performance.

This failure to fulfill the relevant obligations may have various forms of consequences: repeated unavailability or such that it is harmful to normal use; rather long waiting time for the expected response/reaction; disappearance or substantial modification of a feature important to the client without observing the notice period; regression during the update; calculation error; incorrect software documentation that leads to improper use; data for archiving has been requested, but not performed; data archiving has been performed but not completed, so it cannot be reused; loss of the previous archive; the waiting period for the requested service has expired; the presence of viruses in the PDF documents produced by the program; loss or leakage of information about the client's personal or non-personal data after an intrusion into the supplier's system.

It should be noted that there are cases according to which the creditor or customer cannot prove the type of conduct on the part of its debtor (supplier) under the online services agreement: for services provided remotely, the customer cannot check the references, status and experience of the supplier's agents to ensure that they are competent and comply with all the rules; the customer does not have access to technical traces that could prove the supplier's guilt (lack of technical expertise); unclear standards of good practice. Faced with such a situation, two ways can be considered to restore the balance between customers (individuals or professionals) and online service providers, and to facilitate the repair of damage caused during the use of these services by legal obligations that are ancillary to online service contracts.

The establishment of no-fault liability for online service providers implies that in many areas the compensatory function of civil liability takes precedence over all other considerations and has led to a shift to no-fault liability: fault is no longer always required to justify liability.

The above makes it clear that the new possibilities of mass data processing provided by digital enterprises through algorithmic processing obviously have a significant impact on

consumer rights. It is the influence which will allow the EU to create new conditions for consumer protection over time.

Analyzing further the legal liability and the consideration of administrative and financial sanctions, it is important to note that the liability of digital enterprises is accompanied by certain regulations addressed to government agencies, businesses, trade unions, researchers, and stakeholders. The main point I would like to make is that technological progress brings many threats to humanity related to the ongoing digitization process, especially inappropriate or unethical digital practices. These threats primarily concern the global labor market and are associated with the gradual elimination of jobs in both industry and services. Robots are already replacing human work in simple, repetitive activities, and in the long term, machines with artificial intelligence and "deep learning" are expected to develop dynamically, allowing machines to perform functions that also require thinking. This will undoubtedly lead to the elimination of many professions that were previously performed only by humans. Although in the long run new technologies will also create new jobs, some of them in sectors we cannot yet imagine, the general belief of both experts and society is that technology will take away more jobs than it will create.

The process of replacing human labor with machines will entail social and economic costs that are difficult to estimate today and will be borne by individuals and state governments alike. Moreover, not everyone will be able to adapt to the rapidly advancing digital revolution, which requires technological, engineering, or software competencies, which may lead to the progressive digital exclusion of individuals or entire social groups. For workers, digital mobile and communication technologies that offer the possibility of greater flexibility in work may mean an increased demand for constant availability of workers, irregular working hours, blurring of work-life boundaries and offering precarious forms of employment, and may therefore lead to increased levels of stress, exhaustion, life dissatisfaction, as well as weakened connections and isolation. The use of modern digital technologies also involves ethical dilemmas related to humanely important issues such as privacy, free will, autonomy and dignity.

Faced with the challenges associated with the development and implementation of digital technologies, organizations need to better understand how to manage the risks associated with them and find an ethical compass on how to act digitally responsibly towards all stakeholders. Thus, there is a gradual expansion of the concept of corporate social responsibility (CSR) with its new dimension - corporate digital responsibility (CDR). However, this will not solve the problem of the fact that today much of the work in the digital

sphere is done by artificial intelligences, and over time, this will cause unemployment among the relevant segments of the population.

Thus, responsibility for digital enterprises is quite important at the societal level, ensuring socially responsible changes for employees and society, which are increasingly digitalized. Referring to business ethics, corporate digital responsibility can be defined as a set of values and specific norms that govern an organization's judgments and decisions in matters that are specifically digital. It is based on the belief that organizations that develop technology and those that use technology in their operations have an obligation to do so in a way that has a fundamentally positive impact on the enterprise and all its stakeholders. This concept, on the one hand, involves countering the threats that result from advancing digitalization, but on the other hand, it also focuses on seizing the opportunities it brings.

It is important to note that in addition to the above legal liability, there are the following types of liability in the field of digital technologies. In my opinion, the following types of liability also apply to the protection of digital human rights. The content of this type of responsibility relates to the organization's relationship with people and society, covering issues such as ensuring the protection of private data of employees, customers and other stakeholders, promoting digital diversity and digital integration, and applying ethical social practices; economic digital responsibility, reflected in the issue of replacing human jobs with robots and other digital technologies, as well as the issue of sharing the economic benefits of digitalization with businesses and society (e.g., through taxation of digital work) and respecting property rights (e.g., by limiting piracy); technological digital responsibility, which is related to the responsible creation of technologies themselves: ensuring that the algorithms created are ethical, fair and non-discriminatory, and that they are not harmful to society; environmental digital responsibility, which is expressed, for example, in the responsible recycling or disposal of old computer equipment, or in reducing electricity consumption.

More and more digital enterprises are recognizing the need to comprehensively incorporate digitalization into their operational strategies, as evidenced by the voluntary establishment of internal guidelines in companies to address the complexities of digitalization. We can predict that in the future, responsibility will become a distinguishing feature for organizations in both the consumer and employee markets. Particular attention should also be paid to such aspects as user and customer data protection, electronic commercial communications, procedures for appeal and withdrawal of consent, harassment of advertising, unfair competition, the right to be forgotten, the use of cookies, etc.

Thus, legal liability is one of the most important guarantees of observance of human and civil rights and freedoms, which solves the main tasks of ensuring social stability, protecting society from criminal attacks, strengthening and protecting the state. The main liabilities that digital enterprises are held liable for human rights violations include: joint and several liability, contractual and corporate digital legal liability, digital social, economic, technological and environmental legal liability, and fault liability.

CONCLUSIONS

1. International law on human rights and their protection is ensured not only by joint international treaties or agreements adopted by the EU, but also by the domestic legislation of each individual EU member state. In today's realities, human rights should be considered as requirements addressed to both the state and its relevant bodies and enterprises, in accordance with the issue under study, to digital enterprises.

Thus, in the digital space, it is the digital rights whose realization and protection are closely related to the use of online components and digital tools, as well as those that arise in the course of digital activities and claim to be significant in the digital space that need to be protected first. The basic digital human rights include such fundamental rights as freedom of expression and speech, confidentiality (privacy), the right to information and to participate in the management of public affairs, the right to be forgotten and to anonymity, and the right to the Internet.

Along with this analysis of the case law of the EU Court of Justice and the ECHR, it was found that each individual case is considered separately, all factors are weighed for a full and legal resolution of the case on the merits.

2. Digital licensing of businesses plays an important role in the human rights protection system. To date, all EU member states have aligned their national legislation to a comprehensive, full-fledged system of regulating digital licensing and protecting human rights from the state. The main components of a license, which are necessary to guarantee users their digital rights, include legal obligations when purchasing a license: the subject of the contract, the scope of use, the duration of the license, the fee, liability and warranty.

3. Registration processes are quite significant for the protection of human rights, as they can quickly identify a digital enterprise and respond promptly in case of human rights violations, allow the state and state bodies to control the activities of digital enterprises (where the most vulnerable are consumer rights, intellectual property rights, etc.). Also, digital enterprises have access to state services and programs, which regulates the opportunities of all digital market participants, as everyone has the right to engage in this type of activity.

4. In today's conditions, the implementation of privacy and security of personal data of consumers by digital enterprises is important and quite relevant, since digital enterprises are a kind of database that stores significant amounts of user information, such as name, address, telephone number, user's email, personal correspondence, etc.

Considering the EU regulatory framework for the protection of personal data of consumers, the following laws can be noted, namely:

1) General regulation on data protection, which provides rules for digital enterprises that collect, use and store personal data of consumers in their activities;

2) the Directive on electronic commerce, which sets out the rules on how businesses should collect and use personal information of consumers in their activities;

3) the Directive on Privacy and Electronic Communications, which sets out the rules for how digital businesses should collect and use consumer personal information in electronic communications.

5. European legislation quite positively regulates all possible rights of individuals in the digital sphere to ensure the proper realization of the right to freedom of thought, privacy (protection of personal information in the digital sphere), the right to accessibility (access to information), the right to form and join any associations, the right to equal treatment of everyone regardless of their race, gender, sexual orientation, religious preferences, etc. In other words, if a person properly exercises his or her rights in the digital space, there is a clear and comprehensive system of European protection. In my opinion, European legislation reliably protects the personal data of its consumers, but it is worth keeping abreast of the pulse, as unfortunately, fraudulent ones are also developing more and more today, which will eventually lead to the necessary changes in legislation and the introduction of new systems.

6. Administrative and financial sanctions applied to digital enterprises in case of violation of human rights by the latter have a number of features and relevance, as they ensure the norms of substantive and procedural rights, the repressive nature of financial penalties and administrative fines, which are important elements in the system of protection of human rights and freedoms and ensure the necessary efficiency.

When imposing administrative and financial penalties, the relevant governing bodies strictly adhere to the principles of a democratic state governed by the rule of law, equality before the law, proportionality, efficiency and systematization.

The main types of sanctions studied include: increased or penalty fee, additional amount, additional tax liability, financial penalty, non-monetary sanctions.

When imposing sanctions, the governing body is guided by the criterion of the certainty of the offender, for example, if the offender is an individual, the lowest amount of punishment will be applied, and in the case of a state body - the maximum penalty.

The peculiarities of sanctions are that the imposed sanction may be appealed or the required amount paid is divided into separate payments, the interest on which is charged separately.

7. Legal liability is one of the most important guarantees of respect for human and civil rights and freedoms, which solves the main tasks of ensuring social stability, protecting society from criminal attacks, strengthening and protecting the state, in civil, criminal and administrative jurisdiction.

The main types of liability, both legal and digital, to which digital enterprises are held for human rights violations include: joint and several liability, contractual and corporate digital legal liability, digital social, economic, technological and environmental legal liability, as well as fault liability.

LIST OF REFERENCES

I. Scientific literature.

1. Pankratova V.O., Shein D.S. Human rights in the age of information technology. Legal Scientific Electronic Journal No. 3/2021 P. 34-37.

2. Yogesh K. Dwivedi , Elvira Ismagilova, D. Laurie Hughes, Jamie Carlson, Raffaele Filieri, Jenna Jacobson, Varsha Jain, Heikki Karjaluoto, Hajer Kefi, Anjala S. Krishen, Vikram Kumar, Mohammad M. Rahman, Ramakrishnan Raman, Philipp A. Rauschnabel, Jennifer Rowley, Jari Salo, Gina A. Tran, Yichuan Wang Setting the future of digital and social media marketing research: Perspectives and research propositions Available at: https://www.sciencedirect.com/science/article/pii/S0268401220308082

3. Staniszewska, L. (2017). Aligning administrative fines with democratic principles the rule of law (in:) New procedural institutions in administrative proceedings in the light of the amendment Code of Administrative Procedure of April 7, 2017, ed. Gronkiewicz A., Ziółkowska A Katowice.

4. Błachucki, M. (2015). Administrative fines in a democratic state of law. Warsaw.

5. Fedorenko T.V., S.P. Sadkovsky Legal responsibility in the information sphere: concept and features // Journal of Kyiv University of Law: Problems of civil, economic, labor and social security law. Issues 2-4. 2022. C. 82- 85.

6. Uvarova O.O., Buryakovska K.O. Business and human rights: a textbook. Kyiv. 2019. 148 c.

7. Khrystova H. Respect and protection of human rights: main challenges and obligations of the state // Visegrad Journal on Human Rights. 2018. № 5. C. 130-135.

8. Hristova H. Positive obligations of the state in the field of human rights: modern challenges: a monograph. Kharkiv: Pravo, 2018. 500 c.

9. Kirichenko O.V. Conference on Security and Cooperation in Europe // Encyclopedia of Modern Ukraine. URL : https://esu.com.ua/article-71277 .

10. Human Rights: International Law and National Legislation / edited by Prof. V.V. Phillipov. Vilnius, 2011. 338 c.

11. Alexi R. Institutionalization of human rights in a democratic constitutional state. Philosophy of Human Rights; edited by S. Gosepat and G. Lohmann; translated from German by O. Yudin and L. Doronicheva: Nika-Center. Kyiv. 2008. c. 172-190.

12. The right to privacy: conditio sine qua non / Kharkiv Human Rights Protection Group. Kharkiv: Folio, 2003. 216 c.

13. Milanovic M. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age // Harvard International Law Journal. 2015.Vol. 56.N. 1.P. 81–146.

14. Derevyanko V.V., Vasylchenko V.M. Human rights in the digital information space: Collection of materials. 2nd Scientific and Met. Seminar "Human Rights: Reflection in the Media Space". Kyiv. 2023. C. 55-57.

II. Regulatory and legal acts

15. Universal Declaration of Human Rights https://www.un.org/sites/un2.un.org/files/2021/03/udhr.pdf

16. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj

17. Convention on Road Traffic Geneva, 19 September 1949. Available at: https://treaties.un.org/pages/ViewD etailsV. aspx?src=TREATY&mtdsg_no=XI-B-1&chapter=11&Temp=mtdsg5&clang=en

18. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:e

19. Case C-298/07: Judgment of the Court (Fourth Chamber) of 16 October 2008 (reference for a preliminary ruling from the Bundesgerichtshof — Germany) — Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v deutsche internet versicherung AG (Directive 2000/31/EC) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CA0298

20. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC https://eur-lex.europa.eu/eli/dir/2019/790/oj

21. Gesetz über Urheberrecht und verwandte Schutzrechte https://www.gesetze-im-internet.de/urhg/

22. Vertragsrecht für Nichtjuristen http://www.avio-law.de/re sources/Vertragsrecht_fuer_Nichtjuristen.pdf

23. General Data Protection Regulation (EU GDPR) https://gdpr-text.com/

24. Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017. Available at: https://eur-lex.europa.eu/legal-content/E N/TXT/?uri= celex%3A32017L1132

25. United Nations Guiding Principles on Business and Human Rights. Available at: https://www.undp.org/india/publications/united-nations-guiding-principles-business-and-hum

an-rights?gad_source=1&gclid=Cj0KCQiAyeWrBhDDARIsAGP1mWSCSROscdZNxxVdCa1cZ_7RDwEtdfSjDg2aHQgS8paT43BUhj0kdJcaAoHqEALw_wcB

26. Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States (Adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies). Available at:

https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/aDXmrol0vvsU/content/recommendation-cm-rec-2014-6-of-the-committee-of-ministers-to-member-states-on-a-guide-to-human-rights-for-Internet-users-adopted-by-the-committee-of-

27. Treaty on European Union (TEU) / Maastricht Treaty). Available at: https://www.europarl.europa.eu/about-parliament/en/in-the-past/the-parliament-and-the-treaties/maastricht-treaty

28. Communication from the Commission to the European Parliament, the European Council and the Council. Available at: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-02/SWD_2023_30_Ukraine.pdf

29. Consolidated version of the Treaty on the Functioning of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

30. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on protection of natural persons with regard to the processing of personal data and on free movement such data and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L. of 2016, No. 119, page 1, as amended. d.).

31. 39 Act of May 10, 2018 on the protection of personal data (consolidated text: Journal of Laws of 2019, item 1781).

32. Justification of the government bill on the protection of personal data, form 2410. Retrieved from http:// www.sejm.gov.pl/.

33. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781).

34. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2020 r. poz. 256)

35. Act of April 7, 2017 amending the Act - Code of Administrative Procedure and certain other acts (Journal of Laws of 2017, item 935).

36. Uzasadnienie rządowego projektu ustawy o zmianie ustawy - Kodeks postępowania administracyjnego oraz niektórych innych ustaw, druk 1183. Retreived from https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=1183

37. Uzasadnienie rządowego projektu ustawy o ochronie danych osobowych, druk 2410. Retreived from http:// www.sejm.gov.pl/.

38. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483 z późn. zm.).

39. Wyrok NSA z dnia 10 marca 2010, sygn. I FSK 31/08, LEX nr 537191. https://lexlege.pl/orzeczenie/181705/i-sa-ld-378-13-wyrok-wojewodzki-sad-administracyjny-w -lodzi/

40. Wyrok NSA z dnia 2 marca 2016, sygn. II FSK 2474/15, LEX nr 2017629. https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/ii-fsk-2474-15-ulga-w-splacie-zobowiazan-podatkowych-522111325

41. L'idée de créer un droit européen des contrats remonte à 2001. Voir par exemple https://www.senat.fr/rap/l17-022/l17-0223.html

42. Cf. 2.1.1 pour la définition du contrat d'adhésion. https://www.labase-lextenso.fr/revue-des-contrats/RDC115z0

43. Cet article 1171 est issu de la réforme du droit des contrats de 2016. https://www.lettredesreseaux.com/P-1826-451-A1-le-nouveau-droit-des-contrats-d-adhesion.html

44. Article R212-1 pour les clauses abusives de manière irréfragable (le fournisseur n'est pas admis à apporter une preuve contraire) et article R212-2 pour les clauses présumées abusives (le fournisseur doit montrer que la clause n'est pas abusive). https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006069565/LEGISCTA000032807194/

45. Notamment entre les fournisseurs et la grande distribution https://www.lepoint.fr/politique/consommation-une-loi-renforce-les-fournisseurs-face-a-la-grande-distribution-22-03-2023-2513152_20.php

46. L'ancien article L442-6-I du Code de Commerce énumérait 13 pratiques restrictives de concurrence. Le nouvel article L442-1-I n'en liste plus que deux à la suite de l'ordonnance n°2019-359 du 24 avril 2019 portant refonte du titre IV du livre IV du Code de commerce, car cette liste de 13 pratiques restrictives n'était pas pleinement exploitée par les acteurs économiques https://www.legifrance.gou v.fr/codes/article_lc/LEGIARTI000038414237

47. Article 1240 (anciennement 1382) du Code civil. https://www.legifrance.gouv.fr/codes /article_lc/LEGIARTI000032041571

48. Article 1147 Code civil. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006436401/1986-01-01

49. Universal Declaration of Human Rights: UN General Assembly Resolution 217 A (III) of December 10, 1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text.

50. International Covenant on Civil and Political Rights: UN General Assembly Resolution 2200A (XXI) of December 16, 1966.

51. International Covenant on Economic, Social and Cultural Rights: UN General Assembly Resolution A/RES/2200 A (XXI) of December 16, 1966.

52. Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No. 11 and 14. https://rm.coe.int/1680063765

53. European social standard. https://www.coe.int/en/web/european-social-charter

54. Final Act of the Conference on Security and Cooperation in Europe: UN General Assembly Resolution of August 01, 1975. https://zakon.cc/law/document/read/994_055

55. Final Document of the Vienna Meeting of the Representatives of the participating States in Europe of January 15, 1989. http://nbuv.gov.ua/UJRN/Ukrr_1996_3_16

56. Document of the Copenhagen Meeting - Conference on the Human Dimension of the CSCE of June 29, 1990. https://www.osce.org/ru/odihr/elections/14304

57. O'Brien C. M. Business and human rights: a handbook for legal practitioners / Council of Europe, 2018. URL: https://www.coe.int/en/web/nationalimplementation/publications/handbo oks?fbclid=IwAR29oo9XI_6Jj9A6dhHmGTDp7RzoQX5vBueoH-o8I1MPjBxpcdGI9E-zSc

58. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

59. Bărbulescu v. Romania [2017] ECHR 754. https://hudoc.echr .coe.int/eng#{%22itemid%22:[%22001-159906%22]}

60. Rosneft in March 2017 ECLI:EU:C:2017:236 https://curia.europa.eu/juris/document/document.jsf?text=&docid=189262&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7972231

61. Bank Refah Kargaran In Case C134/19 P https://curia.europa.eu/juris/document/document.jsf?text=&docid=232086&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=7972061

62. Razmetayeva Y.S. Digital human rights and problems of extra-territoriality in their protection: Law and Public Administration. Issue 4 2020. C. 18-23.

63. EU Charter of Fundamental Rights https://ecas.org/eu-rights/?gad_source=1&gclid=Cj0KCQiAyeWrBhDDARIsAGP1mWRJBjuu6ySuDR940XJWiUYXlNHydOoR8fB8nWcnTrKEsYOipWsJ7goaAhStEALw_wcB

64. Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 ('Directive on electronic commerce') https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031

65. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (Directive on privacy and electronic communications) https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

66. Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law https://www.europeanpapers.eu/en/europeanforum/google-v-cnil-territorial-scope-of-right-to-be-forgotten-under-eulaw#:~:text=In%20its%20landmark%20ruling%20in,right%20to%20be%20forgotten%20globally

67. Common Foreign and Security Police https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/common-foreign-and-security-policy_en

68. Digital Markets Act and the Digital Services Act https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

III. Internet resources

69. Tesla's Autopilot not responsible for fatal 2019 crash in California, jury finds in landmark case https://www.cbsnews.com/news/tesla-autopilot-not-responsible-fatal-2019-crash-california-jury-finds-landmark-case/

70. Volkswagen: Robot kills worker installing it https://www.dw.com/en/robot-kills-worker-at-volkswagen-plant-in-germany/a-18556982

71. Economic Commission for Latin America and the Caribbean (ECLAC), Digital technologies for a new future (LC/TS.2021/43), Santiago, 2021.

72. Miloš Obrenović. Available at: https://alchetron.com/Milo%C5%A1-Obrenovi%C4%87

73. Унапређен сервис „еРегистрација оснивања привредног друштва“ који омогућује истовремено евидентирање стварног власника (Розширений сервіс «Електронна реєстрація створення приватного підприємства», що дозволяє одночасно зареєструвати реального власника Available at: https://www.apr.gov.rs/%D0%B2%D0%B5%D1%81%D1%82%D0%B8.6.html ?newsId=3696 #

74. Personenbezogene Daten – Wichtige Regelungen im Datenschutz. Available at: https://www.haendlerbund.de/de/ratgeber/recht/4266-personenbezogene-daten

75. Ritu Gill What is Open-Source Intelligence? Available at: https://www.sans.org/blog/what-is-open-source-intelligence/

76. Remedying human rights abuses: a positive role for sustainability systems. Available at: https://www.isealalliance.org/sustainability-news/remedying-human-rights-abuses-positive-role-sustainability-systems

77. Further erosion of the Polish democracy: providing feedback for the first EU Rule of Law Report. Available at: https://en.odfoundation.eu/a/27558,further-erosion-of-the-polish-democracy-providing-feedback-for-the-first-eu-rule-of-law-report/?gclid=CjwKCAjwseSoB hBXEiwA9 iZtxsqCXt-boYCo8TNmt kebToJXh_4zZF_8LAUIGwWruyPOImR5Y cNIJwRoCG7cQAvD_BwE

78. Guidelines for data protection officers ("DPOs"). Retreived from https://uodo.gov.pl/pl/10/7.

79. Żakiewicz-Zborska, K. «Dr Edyta Bielak-Jomaa: Attention, this law applies to everyone». Retreived from

80. By James Sullivan and Fawn Fitter How to make sustainable materials use matter. Available at: https://www.sap.com/central-asia-caucasus/insights/viewpoints/how-to-make-sustainable-materials-use-matter.html

81. The Essentials for Successful Digital Transformation (DX). Available at: https://www.sap.com/central-asia-caucasus/insights/viewpoints/what-are-the-essentials-for-successful-digital-transformation-dx.html

82. The new digital edge: Rethinking strategy for the postpandemic era. Available at: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-new-digital-edge-rethinking-strategy-for-the-postpandemic-era

SUMMARY

Restrictions of the Right to Conduct Business in the Digital Domain in the Interests of Protecting Other Human Rights

Yelyzaveta Nalkovska

The master's thesis analyzes the issues of limiting the right to do business in the digital sphere in the interests of protecting other human rights, including the definition of protection of rights in the digital space, the importance of registration processes, liability for violations of human rights in the digital space, and protection of personal data. The topicality of the master's thesis is revealed in the active manifestation and realization of digital rights by society, the opening of digital businesses, the transition of society to an electronic mode, the active use of artificial intelligence, etc. The above has significantly increased the level of violations of digital human rights, the protection of which is currently well regulated in the EU and its member states.

The thesis analyzes the fundamental human rights in the digital space, the legal acts that regulate them, and also notes the importance of registration processes, problems that arise during registration, and the importance of mandatory business licensing, which is one of the aspects of human rights protection in the digital space. Based on the analysis of legislation and experience of successful countries regarding the protection and security of personal data, the article examines the GDPR and a number of other European legislative sources as the basis for personal data protection. The author characterizes the aspects of personalization and automation of information on the Internet, users' rights and obligations in the event of a personal data breach. The author identifies the types of legal liability and, separately, digital liability arising in the event of a personal data breach. In addition, the peculiarities of administrative and financial sanctions in case of violation of human rights are established.

SUMMARY

Teisės užsiimti verslu skaitmeninėje aplinkoje ribojimas dėl kitų žmogaus teisių apsaugos interesų

Yelyzaveta Nalkovska

Magistro darbe analizuojami teisės užsiimti verslu skaitmeninėje erdvėje ribojimo siekiant apsaugoti kitas žmogaus teises klausimai, įskaitant teisių apsaugos skaitmeninėje erdvėje apibrėžimą, registracijos procesų svarbą, atsakomybę už žmogaus teisių pažeidimus skaitmeninėje erdvėje ir asmens duomenų apsaugą. Magistro darbo tematika atskleidžiama aktyviai pasireiškiant ir įgyvendinant visuomenės skaitmenines teises, atveriant skaitmeninį verslą, visuomenei pereinant į elektroninį režimą, aktyviai naudojant dirbtinį intelektą ir kt. Dėl minėtų aplinkybių labai išaugo skaitmeninių žmogaus teisių, kurių apsauga šiuo metu gerai reglamentuota ES ir jos valstybėse narėse, pažeidimų lygis.

Magistro darbe analizuojamos pagrindinės žmogaus teisės skaitmeninėje erdvėje, jas reglamentuojantys teisės aktai, taip pat atkreipiamas dėmesys į registracijos procesų svarbą, registracijos metu kylančias problemas, privalomo verslo licencijavimo, kuris yra vienas iš žmogaus teisių apsaugos skaitmeninėje erdvėje aspektų, svarbą. Magistro darbe, remiantis teisės aktų analize ir sėkmingai veikiančių šalių patirtimi, susijusia su asmens duomenų apsauga ir saugumu, nagrinėjamas Bendrasis duomenų apsaugos reglamentas (BDAR) ir kai kurie kiti Europos teisės šaltiniai kaip asmens duomenų apsaugos pagrindas. Autorė apibūdina informacijos personalizavimo ir automatizavimo internete aspektus, naudotojų teises ir pareigas asmens duomenų pažeidimo atveju. Autorė nurodo teisinės atsakomybės rūšis ir atskirai skaitmeninę atsakomybę, atsirandančią asmens duomenų saugumo pažeidimo atveju. Be to, nustatomi administracinių ir finansinių sankcijų žmogaus teisių pažeidimo atveju ypatumai.