Monographic Section

DOI: 10.25115/eea.v39i9.5799

Studies of Applied Economics / Estudios de Economía Aplicada

Volume 39-9, September 2021 // ISSN: 1133-3197

Protection of Personal Data According to European Law and Decisions of ECHR

OLHA B. OLIYNYK[1], ALIONA S. ROMANOVA[2], IHOR M. KOVAL[3], OLENA L. CHORNOBAI[4], SVITLANA O. POLIARUSH-SAFRONENKO[5]

[1]Department of State and Legal Disciplines, UNIVERSITY OF ECONOMICS AND LAW "KROK", UKRAINE. E-mail: oliynyk8053@edu-knu.com

[2]Department of Theory and Philosophy of Law, Constitutional and International Law, Institute of Jurisprudence, Psychology and Innovative Education, LVIV POLYTECHNIC NATIONAL UNIVERSITY, UKRAINE

[3]Department of Theory and Philosophy of Law, Constitutional and International Law, Institute of Jurisprudence, Psychology and Innovative Education, LVIV POLYTECHNIC NATIONAL UNIVERSITY, UKRAINE

[4]Department of Theory and Philosophy of Law, Constitutional and International Law, Institute of Jurisprudence, Psychology and Innovative Education, LVIV POLYTECHNIC NATIONAL UNIVERSITY

[5]Department of State and Legal Disciplines, Faculty of Law, UNIVERSITY OF ECONOMICS AND LAW "KROK", UKRAINE

ABSTRACT

This article considers the question of legal basis of the data protection in the world while and exactly in the European continent. Special attention is paid to the question of personal data as a part of human rights and how the ECHR is dealing with protection of it. The author analyzed a list of different type of issues related to the question of personal data and how they are protected under the Article 8 of the ECHR. In conclusion, we proposed some measures that may improve institute of personal data protection in general.

Keywords: Data protection; European Court of Human Rights; Privacy; European Convention of Human Rights; Cyber law.

JEL Classification: K20, K24.

Received: July 07, 2021
Accepted: August 22, 2021

Sección Monográfica

DOI: 10.25115/eea.v39i9.5799

Studies of Applied Economics — Estudios de Economía Aplicada

Volumen 39-9, Septiembre 2021 // ISSN: 1133-3197

Protección de Datos Personales de Acuerdo con la Ley Europea y las Decisiones del CEDH

OLHA B. OLIYNYK[1], ALIONA S. ROMANOVA[2], IHOR M. KOVAL[3], OLENA L. CHORNOBAI[4], SVITLANA O. POLIARUSH-SAFRONENKO[5]

[1]Department of State and Legal Disciplines, UNIVERSITY OF ECONOMICS AND LAW "KROK", UKRAINE. E-mail: oliynyk8053@edu-knu.com

[2]Department of Theory and Philosophy of Law, Constitutional and International Law, Institute of Jurisprudence, Psychology and Innovative Education, LVIV POLYTECHNIC NATIONAL UNIVERSITY, UKRAINE

[3]Department of Theory and Philosophy of Law, Constitutional and International Law, Institute of Jurisprudence, Psychology and Innovative Education, LVIV POLYTECHNIC NATIONAL UNIVERSITY, UKRAINE

[4]Department of Theory and Philosophy of Law, Constitutional and International Law, Institute of Jurisprudence, Psychology and Innovative Education, LVIV POLYTECHNIC NATIONAL UNIVERSITY

[5]Department of State and Legal Disciplines, Faculty of Law, UNIVERSITY OF ECONOMICS AND LAW "KROK", UKRAINE

RESUMEN

Este artículo considera la cuestión de la base jurídica de la protección de datos en el mundo mientras y exactamente en el continente europeo. Se presta especial atención a la cuestión de los datos personales como parte de los derechos humanos y cómo el CEDH trata su protección. El autor analizó una lista de diferentes tipos de cuestiones relacionadas con la cuestión de los datos personales y cómo están protegidos en virtud del artículo 8 del CEDH. En conclusión, propusimos algunas medidas que pueden mejorar el instituto de protección de datos personales en general.

Palabras clave: Protección de datos; Tribunal Europeo de Derechos Humanos, Privacidad; Convenio Europeo de Derechos Humanos, Derecho cibernético.

Clasificación JEL: K20, K24.

Recibido: 07 de Julio de 2021
Aceptado: 22 de Agosto de 2021

1. Introduction

Problem of human rights protection arises each year bigger. Now the question of rights and freedoms of human and citizen is the main problem of national and international communities. It has raised a special attention since last century, when a lot of countries started their course of democratization (Gonzalez Fuster, 2016). Ensuring human rights and freedoms and their practical implementation are the standards for assessing the level of democratic development of any country. One of the most vulnerable species of human rights is data protection rights (Komkova et al., 2020; Novikovas et al., 2017). We are providing our personal data online, sometimes knowing and unknowing about this, for many various reasons, as e-learning, playing, e-shopping or while using social networks. Internet with all its tools made our life much easier than it was before, but in the same moment it brought a lot of dangerous for our privacy and personal information.

Personal data has become one of the main bloodlines in our lives, the same as has the significance of rules regulating it in some form. The one of the first try to regulate personal data protection was made by the Council of Europe in 1981 when Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, known as "Convention 108", was adopted. This treaty is still one of the main and the only international documents which applies to all binding international instrument in the data protection field. According to Lydia de la Torre, professor at Santa Clara University, the key points of Convention 108 are:

- Outlaws, in the absence of proper legal safeguards, the processing of 'sensitive' data – such as on a person's race, politics, health, religion, sexual life or criminal record.
- Enshrines the individual's rights that align with EU data protection law, including the right to know that information is stored and the right to have it corrected.
- Permits restrictions on the rights laid down in the convention only when overriding interests, such as state security or defense, are at stake; and
- Provides for the free flow of personal data between its Contracting Parties but allows for restrictions on flows to states where legal regulation does not provide adequate protection (de la Torre, 2019).

Convention 108 right now is open for accession by non-Contracting Parties of the Council of Europe, what is giving a chance for this treaty to be come first unified international document in data protection. Except of all advantages this Convention has, there is still one big problem. Convention 108 is binding for states that have ratified it but it is not subject to the judicial supervision of the European Court of Human Rights (the ECHR).

In 1950, the Council of Europe adopted the European Convention of Human Rights (the Convention). Contracting Parties to this Convention have an international obligation to comply with it, which is enforced through the European Court of Human Rights (Oganesian, 2020; Yaroshenko et al., 2018). The Convention does not directly provide protection of personal data, but through the Article 8 it guarantees the right to respect for private and family life, home and correspondence, and lays down the conditions under which restrictions of this right are permitted, what is some way also covers issues of data protection.

The ECHR has examined many situations involving data protection issues: interception of communications,16 various forms of surveillance by both the private and public sectors, and protection against storage of personal data by public authorities. According to the statistics of the court of 2020, article 8 is one of the most violated articles in 2020 (93 cases). The respect for private life is not an absolute right, as the exercise of the right to privacy could compromise other rights, such as freedom of expression and access to information and vice versa. Hence, the Court strives to find a balance between the different rights at stake. It has clarified that Article 8 of the ECHR not only obliges states to refrain from any actions that might violate this convention right, but that they are in certain circumstances also under positive obligations to actively secure effective respect for private and family life.

2. Methodology

The methodological basis of the research included general scientific methods: dialectic, logical, system, statistic, etc. There were also used some specifically methods of the international law science: the system-legal methods, the comparative-legal methods and the methods of interpretation of law. The huge number of the decisions of the ECHR require to use the system-legal method. This method helps to organize process of legal analyzing of cases, which allows to find important facts that made influence on the data protection law. The same as classic system method, which helps to make the right order of all important documents for personal data and human rights in this sphere, it provides a special chronology of regulation.

The comparative-legal method gives an opportunity to find out how the data protection law has changed since 1981, when Convention 108 was created, and what was the influence on human rights so fast and big digitalization during the last decades (European Union Agency for Fundamental Rights and Council of Europe, 2018). And the method of interoperation of law will help us to see how through the paradigm of the ECHR decisions was changed the level of safety of human right in field of data protection. It is also important to mention about the chronological methodology. This method determines the sequence of legal acts, court practices, which regulate the protection of personal data. With this method, it become easier to analyze content of the Convention No. 108 and a huge number of judgments of the European Court of Human Rights.

3. Results and discussion

Article 8 of the European Convention of Human Rights guarantees everyone the right to respect for personal and family life, housing and correspondence and prevents interference by public authorities with the exercise. This article does not directly cover the protection of personal data, and this may be easily explained because of the period of time when the Convention was adopted. Since 1950, all world has passed a long and fast way of evolution in technological and information sphere, which requires a new way of regulation of human rights law. But as noted by G. Nardell, the ECHR interprets Paragraph 1 of Article 8 of the Convention quite “generously and widely” (Nardell, 2010). This interpretation due to “modern conditions” allows the ECHR to include the right of data protection to Article 8 of the Convention.

During the last decades, the ECHR has issued decisions on various cases about data protection and each of them provides new specific interpretation of exact problem in sphere of personal data. In the case *“S. and Marper v. the United Kingdom”,* the Grand Chamber of the ECHR gave full answer about why it’s important to separate and categorize each case about data protection: “The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 [of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence] ... The subsequent use of the stored information has no bearing on that finding ... However, in determining whether the personal information retained by the authorities involves any ... private-life [aspect] ..., the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained …”. (S. and Marper v. the United Kingdom, 2008). So, we can make a conclusion about the variety of meanings of “use of personal data”, which it’s important to analyze each kind of cases to see the difference between each type of personal data and how to protect it. (S. and Marper v. the United Kingdom, 2008).

For the beginning, it is important to find the definition of what is understanding under “personal data”. Under the law of the Council of Europe and under European Union (the EU) law “personal data’ is defined as information relating to an identified or identifiable natural person. 6 It concerns information about a person whose identity is either manifestly clear or can be established from additional information. To determine whether a person is identifiable, a controller or another person must take into account all reasonable means that are likely to be used to directly or indirectly identify

the individual, such as, for example, singling out, which makes it possible to treat one person differently from another. If data about such a person are being processed, this person is called the "data subject". By personal data can be understand any kind of information that may be identified. Personal data covers information pertaining to the private life of a person, which also includes professional activities, as well as information about the public life of this person. The ECHR interpreted the term "personal data" as not limited to matters of the private sphere of an individual, according to the Amann case. This meaning is also similar to the one provided by the General Data Protection Regulation (the GDPR) (European Parliament, 2016).

The General Data Protection Regulation is the toughest privacy and security law in the world. It was adopted by the EU in 2018, and its main aim is to impose obligations onto any organization, when they target or collect data related to people in the EU. The GDPR reflected the data protection principles already contained in national laws and in Convention 108, while often expanding them. It drew on the possibility, provided for in Article 11 of Convention 108, of adding on instruments of protection. In particular, the introduction in the directive of independent supervision as an instrument for improving compliance with data protection rules proved to be an important contribution to the effective functioning of European data protection law (European Court of Human Rights, 2018).

Before the GDPR, European Union was already approving one regulation of personal data protection. It was the Directive of 1995. The GDPR maintains the approach of the previous Directive by fixing general principles to be observed in any context of personal data processing, including in research and for archiving purposes in the public interest, and regardless of the kind of personal data, including to the processing of data qualified as sensitive personal data. Nevertheless, the GDPR adds three new general principles of importance (Chassang, 2017). Important fact of the GDPR is that it is only instrument for regulating data protection of EU citizens, what does not cover all European continent. Unlike the GDPR, decisions of the ECHR are mandatory for all state-participants of the Council of Europe, so almost countries of European continent are part of it (except Republic of Belarus), what makes impact and protection of personal data much bigger.

As was mentioned before, the ECHR interprets the meaning of "personal data" according to the specific type of case. Conditionally, after a years of practice, there are such type of protection data cases: interception of communications, phone tapping and secret surveillance; monitoring of employees' computer use; voice samples; video surveillance; storage and use of personal data In the context of criminal justice; storage and use of personal data In the context of health; telecommunication service providers' data; disclosure of personal data; access to personal data; erasure or destruction of personal data.

Interception of communications, phone tapping and secret surveillance is protected under Article 8 of the European Convention on Human Rights. In order to determine whether the interference by the authorities with the applicants' private life or correspondence was necessary in a democratic society and a fair balance was struck between the different interests involved, the European Court of Human Rights examines whether the interference was in accordance with the law, pursued a legitimate aim or aims and was proportionate to the aim(s) pursued. This category is one of the most violated starting from 1978 till 2020.

An ideal example, of violation of Article 8 according to category of Interception of communications, phone tapping and secret surveillance, is case *"R.E. v. the United Kingdom*". The applicant was arrested and detained in Northern Ireland on three occasions in connection with the murder of a police officer. He complained about the regime for covert surveillance of consultations between detainees and their lawyers and between vulnerable detainees and "appropriate adults". The court decided that: "This case was considered from the standpoint of the principles developed by the Court in the area of interception of lawyer-client telephone calls, which call for stringent safeguards. The Court found that those principles should be applied to the covert surveillance of lawyer-client consultations in a police station.

In the present case, the Court held that there had been a violation of Article 8 of the Convention as concerned the covert surveillance of legal consultations. It noted in particular that guidelines arranging for the secure handling, storage and destruction of material obtained through such covert surveillance had been implemented since 22 June 2010. However, at the time of the applicant's detention in May 2010, those guidelines had not yet been in force. The Court was not therefore satisfied that the relevant domestic law provisions in place at the time had provided sufficient safeguards for the protection of the applicant's consultations with his lawyer obtained by covert surveillance." (R.E. v. the United Kingdom, 2015)

But, this case also interesting, because except constating the fact of violation, the ECHR also gave explanation why other part of claims were not held. According to the decision of the court: "The Court further held that there had been no violation of Article 8 as concerned the covert surveillance of consultations between detainees and their "appropriate adults", finding in particular that they were not subject to legal privilege and therefore a detainee would not have the same expectation of privacy as for a legal consultation. Furthermore, the Court was satisfied that the relevant domestic provisions, insofar as they related to the possible surveillance of consultations between detainees and "appropriate adults", were accompanied by adequate safeguards against abuse." So, it was mentioned before, it is important to make a clear legal purpose by state to provide any type of interception of communications, phone tapping and secret surveillance.

The next category is monitoring of employees' computer use, which is perfectly described in *"Barbulescu v. Romania"* case. The case concerned the decision of a private company to dismiss an employee after monitoring his electronic communications and accessing their contents. The applicant complained that his employer's decision was based on a breach of his privacy and that the domestic courts had failed to protect his rights to respect for his private and correspondence. The Grand Chamber held, be 11 votes to 6, that there had been a violation of Article 8 of the Convention. They found that the Romanian authorities had not protected the right to respect private life and correspondence, and they had failed to strike a balance between interests at stake. the national courts had failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications might be monitored; nor had they had regard either to the fact that he had not been informed of the nature or the extent of the monitoring, or the degree of intrusion into his private life and correspondence. (Barbulescu v. Romania, 2017)

A lot of attention was paid by the ECHR to the issues of storage and use of personal data. In case *"S. and Marper v. the United Kingdom"* the Grand Chamber said that: "The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article ... The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored ... [It] must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse ...". This precedent is the basis for the data protection under the Convention and gave first step understanding of "data protection" under the practice of the ECHR. (S. and Marper v. the United Kingdom, 2008).

One of the latest cases on personal data issue is *"Gaughran v. the United Kingdom"*. This case concerned a complaint about the indefinite retention of personal data (DNA profile, fingerprints and photograph) of a man who had a spent conviction for driving with excess alcohol in Northern Ireland. The Court held that there had been a violation of Article 8. The court underlined that the duration of the retention of data is important, it is mandatory to pay attention to certain safeguards. The applicant's personal data had been retained indefinitely without consideration of the seriousness of his offence, the need for indefinite retention and without any real possibility of review. According to

the opinion of the court, the retention of the applicant's data had failed to strike a fair balance between the competing public and private interests (Gaughran v. the United Kingdom, 2020).

One of categories that has a lot of cases is disclose of personal data. The first of cases was *"Z. v. Finland"* in which the applicant's condition as HIV-positive in criminal proceedings were disclosed. The Court held that there had been a violation of Article 8. The disclosure of the applicant's identity and HIV infection, in the text of judgment of the Court of Appeal's which became available to press, had violated the applicant's right to the respect for her private life and family life. The ECHR noted: "…in particular that respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention and is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general." (Z. v. Finland, 1997).

It is also important to talk about access to personal data in the light of the ECHR's decisions. In case *"Turek v. Slovakia"* the applicant alleged in particular that the continued existence of a former Czechoslovak Communist Security Agency file registering him as one of its agents, the issuance of a security clearance to that effect, the dismissal of his action challenging that registration and the resultant effects constituted a violation of his right to respect for his private life. Firstly, we should note that particularly in proceedings related to the operations of state security agencies might access to some information. But in this case, as it was related to the issue of the lustration proceeding, that requirement placed an unrealistic and excessive burden on the applicant and did not respect the principle of equality. There had therefore been a violation of Article 8 of the Convention concerning the lack of a procedure by which the applicant could seek protection for his right to respect for his private life. The Court lastly found it unnecessary to examine separately the effects on the applicant's private life of his registration in the former State Security Agency files and of his negative security clearance. (Turek v. Slovakia, 2006).

The last type of cases that we are going to discuss is erasure or destruction of personal data. In *"Rotaru v. Romania"* the applicant complained that it was impossible to refute what he claimed was untrue information in a file on him kept by the Romanian Intelligence Service (RIS). He had been sentenced to a year's imprisonment in 1948 for having expressed criticism of the communist regime. The ECHR held that there had been a violation of Article 8: "… the holding and use by the RIS of information about the applicant's private life had not been in accordance with the law. The Court observed in particular that public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities…

It further noted that no provision of domestic law defined the kind of information that could be recorded, the categories of people against whom surveillance measures such as gathering and keeping information could be taken, the circumstances in which such measures could be taken or the procedure to be followed. Similarly, the law did not lay down limits on the age of information held or the length of time for which it could be kept… That being so, the Court considered that Romanian law did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities." (Rotaru v. Romania, 2000). In the second part of the decision, it was also mentioned about violation of Article 13 (the right to an effective remedy), because it was impossible for the applicant to challenge the data storage or to refute the truth of the information in question.

4. Conclusion

At present the European Court of Human Rights is one of the main international human rights institutions of European system of protection of human rights, which is also providing special adjudication settlement of disputes about data protection. The European Court of Human Rights with its decisions and given recommendations influences on formation, reforming of contemporary national and international personal data protection sphere, practical use of European legal standards in making decisions by national courts. It should be emphasized that decisions of the European Court of Human

Rights are obligatory for member states, and their execution is controlled by the Committee of Ministers of the Council of Europe, but this rule is not applying to the whole world. That is why, one of the most important things which world should provide to the world is some general way how to protect and settle disputes about personal data.

To sum up, we should pay attention to the question of data protection. The age of internet and informational technologies develops so fast, that right now we have more and more issues of personal data violation. It is primary important in the question to the right of privacy and family life, which is granted by the European Convention on Human Rights, and which are violated so much. There are a couple of reasons why it is like this. Firstly, there is no one completely unique world document that will cover this question. European continent developed a couple of treaties that covered issue of data protection in Europe, but they do not completely help for the whole world. Both the GDPR and the Convention 108 are examples of good legislation in personal data. Each of them helps to understand basic rules and gives unified explanation for the meaning and importance of data protection.

Secondly, there are not so many institutions that will help to protect your rights if they will be violated. The ECHR has a lot of cases on the protection of data, but the European Convention on Human Rights does not cover fully the question of personal data. One of the main advantages of the ECHR decision that they classified them according to the type of data protection. Each case of the ECHR brings new precedent to the protection of personal data, what is basically a new law. That is good because the decisions of the ECHR are the law that develops according to the modern time and needs. It is important to develop precedent law on data protection on other parts of the word, so this sphere will be more protected.

Taking into account all the issues and points about protection of personal data that were mentioned in this article, we can constant the fact that data protection is only on the stage of development. We already have some valuable documents which provides some king of guarantees for humans about protection of their rights for privacy, but we still need to look for the new ways how to save human rights from any kind of violation, and to be ready for new problems with which we may meet in the nearest future. As the Commissioner for human rights in Council of Europe, Dunja Mijatovic, said: “It is extremely important to find the right balance between technological development and the protection of human rights, because the future of the society in which we want to live will depend on it.”

References

1. Barbulescu v. Romania (2017). No. 61496/08, 5 September 2017. Retrieved from https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-177082%22]}
2. Chassang, G. (2017). The impact of the EU general data protection regulation on scientific research. Retrieved from https://ecancer.org/en/journal/article/709-the-impact-of-the-eu-general-data-protection-regulation-on-scientific-research#:~:text=According%20to%20this%20techno%2Dlegal,by%20the%20processing%2C%20the%20controller
3. De la Torre, L. (2019). What is “Convention 108”. Retrieved from https://medium.com/golden-data/what-is-coe-108-3708915e9846
4. European Court of Human Rights. (2018). Guide of the European Convention on Human Rights. Retrieved from https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb
5. European Parliament. (2016). The General Data Protection Regulation. Retrieved from https://gdpr-info.eu/
6. European Union Agency for Fundamental Rights and Council of Europe. (2018). Handbook on European data protection law. Retrieved from https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf

7. Gaughran v. the United Kingdom (2020). No. 45245/15, 13 February 2020. Retrieved from https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-200817%22]}
8. Gonzalez Fuster, G. (2016). *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer.
9. Komkova, G. N., Basova A. V., & Torosyan R. A. (2020). Constitutional protection of public figures' personal data on the Internet. *Journal of Siberian Federal University. Humanities & Social Science, 13*(1), 68-75.
10. Nardell, Q.C.G. (2010). Levelling up: data privacy and the European Court of Human Rights. In Serge Gutwirth, Yves Poullet, & Paul De Hert (Eds.), *Data Protection in a Profiled World* (pp. 43-52). Dordrecht: Springer.
11. Novikovas, A., Novikoviene, L., Shapoval, R., & Solntseva, K. (2017). The peculiarities of motivation and organization of civil defence service in Lithuania and Ukraine. *Journal of Security and Sustainability Issues, 7*(2), 369-380.
12. Oganesian, T. D. (2020). The right to privacy and data protection in the information age. *Journal of Siberian Federal University. Humanities & Social Science, 13*(10), 1576-1588.
13. R.E. v. the United Kingdom (2015). No. 62498/11, 27 October 2015. Retrieved from https://www.statewatch.org/media/documents/news/2015/oct/ecxhr-judgment-full-text-R-E--v-UK-covert-surveillance-of-detainees'-consultations.pdf
14. Rotaru v. Romania (2000). No. 28341/95, 4 May 2000. Retrieved from http://www.hraction.org/wp-content/uploads/Rotaru_protiv_Rumunije.pdf
15. S. and Marper v. the United Kingdom (2008). No. 30562/04 and 30566/04, 4 December 2008. Retrieved from https://rm.coe.int/168067d216
16. Turek v. Slovakia (2006). No. 57986/00, 14 February 2006. Retrieved from http://melaproject.org/sites/default/files/2019-01/ECtHR%2C%20Turek%20v.%20Slovakia%20%28Appl.%20No.%2057986%3A00%29%2C%20Judgment%2C%2014%20February%202006.pdf
17. Yaroshenko, O. M., Moskalenko, O. V., Sliusar, A. M., & Vapnyarchuk, N. M. (2018). Commercial secret as an object of labour relations: Foreign and international experience. *Journal of Legal, Ethical and Regulatory Issues, 21*(Special Issue 1).
18. Z. v. Finland (1997). No. 22009/93, 25 February 1997. Retrieved from https://www.staff.uni-mainz.de/kebert/Entscheidungen/EGMR%20Z%20v%20Finland.pdf