Revista JURÍDICA PORTUCALENSE

www.upt.pt

IJP PORTUCALENSE INSTITUTE FOR LEGAL RESEARCH

FCT Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA EDUCAÇÃO E CIÊNCIA

N.º 33 | Universidade Portucalense | Porto | 2023

https://doi.org/10.34625/issn.2183-2705(33)2023

Olha B. Oliynyk, Aliona S. Romanova, Ihor M. Koval, Olena L. Chornobai, Svitlana O. Poliarush-Safronenko

Protection of Personal Data in the Context of Human Rights: Experience and Relevance of ECtHR Decisions

DOI: https://doi.org/10.34625/issn.2183-2705(33)2023.ic-10

Secção I

Investigação Científica*

* Os artigos presentes nesta secção foram sujeitos a processo de revisão segundo o método *blind peer review*.

Protection of Personal Data in the Context of Human Rights: Experience and Relevance of ECtHR Decisions

Proteção de Dados Pessoais no Contexto dos Direitos Humanos: Experiência e Relevância das Decisões do TEDH

Olha B. OLIYNYK[1]
Aliona S. ROMANOVA[2]
Ihor M. KOVAL[3]
Olena L. CHORNOBAI[4]
Svitlana O. POLIARUSH-SAFRONENKO[5]

ABSTRACT: The article aims to examine the legal framework for data protection in the European continent. The article analyzes the issue of personal data through the prism of human rights and their protection under Article 8 of the European Convention on Human Rights. The article analyzes the ECtHR experience and the relevance of its decisions in the context of the protection of personal data. The authors study the legal understanding of personal data within European law. The legal basis for the protection of personal data was analyzed, and new mechanisms that could be used under the fast development of information technologies were established. All these questions lead to the idea that there is no unique and universal way to protect personal data, even though it is required, given the high level of cyberterrorism. In this article, the authors attempt to find a universal mechanism for regulating access to personal data and protecting it on the international level by public and private international law. In conclusion, a set of measures that can improve the institute of personal data protection is suggested.
KEYWORDS: human rights; legal regulation; personal data; privacy; right to respect for private life.

RESUMO: O artigo tem como objetivo examinar o marco legal da proteção de dados no continente europeu. O artigo analisa a questão dos dados pessoais sob o prisma dos direitos humanos e sua proteção nos termos do artigo 8º da Convenção Europeia dos Direitos Humanos. O artigo analisa a experiência do TEDH e a relevância de suas

[1] Department of State and Legal Disciplines, Faculty of Law, University of Economics and Law "KROK", 03113, 30-32 Tabirna Str., Kyiv, Ukraine.
[2] Department of Theory and Philosophy of Law, Constitutional and International of Law, Educational and Scientific Institute of Law, Psychology and Innovative Education, Lviv Polytechnic National University 79000, 12 Stepana Bandera Str., Lviv, Ukraine.
[3] Department of Theory and Philosophy of Law, Constitutional and International Law, Institute of Jurisprudence, Psychology and Innovative Education, Lviv Polytechnic National University, 79013, 12 Bandera Str., Lviv, Ukraine.
[4] Department of Theory and Philosophy of Law, Constitutional and International Law, Institute of Jurisprudence, Psychology and Innovative Education, Lviv Polytechnic National University 79013, 12 Bandera Str., Lviv, Ukraine.
[5] Department of State and Legal Disciplines, Faculty of Law, University of Economics and Law "KROK" 03113, 30-32 Tabirna Str., Kyiv, Ukraine.

decisões no âmbito da proteção de dados pessoais. Os autores estudam o entendimento legal de dados pessoais dentro da legislação europeia. A base legal para a proteção de dados pessoais foi analisada, e novos mecanismos que poderiam ser utilizados no contexto do rápido desenvolvimento das tecnologias de informação foram estabelecidos. Todas essas questões levam à ideia de que não existe uma forma única e universal de proteger os dados pessoais, ainda que seja necessária, dado o alto nível de ciberterrorismo. Neste artigo, os autores tentam encontrar um mecanismo universal para regular o acesso aos dados pessoais e protegê-los em nível internacional pelo direito internacional público e privado. Em conclusão, sugere-se um conjunto de medidas que podem melhorar o instituto da proteção de dados pessoais.
PALAVRAS-CHAVE: direitos humanos; regulamentação legal; dados pessoais; privacidade; direito ao respeito pela vida privada.

1. Introduction

The problems of protection of human rights are growing annually. Human rights and freedoms are the main problems of national and international communities. These problems raised special attention in the last century when numerous countries started their course for democratization[6]. 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 human rights is data protection rights[7].

People provide their personal data online (consciously or unconsciously) for e-learning, playing, shopping online, or using social networks. The Internet and all its tools made our life much easier; however, the Internet also brought numerous dangers to our privacy and personal information.

- The Council of Europe made the first attempt to regulate personal data protection when it adopted the Convention for the Protection of Individuals in 1981 with regard to Automatic Processing of Personal Data, known as "Convention 108." This treaty is still one of the main and the only international documents which applies to all binding international instruments in the data protection field. According to Lydia de la Torre, a professor at Santa Clara University, the key points of Convention 108 are as follows:

[6] GONZALEZ FUSTER, G. *The emergence of personal data protection as a fundamental right of the EU*. Cham: Springer, 2016.
[7] KOMKOVA, G. N., BASOVA A. V., and TOROSYAN R. A. Constitutional protection of public figures' personal data on the Internet. *Journal of Siberian Federal University. Humanities & Social Science*, 2020, vol. 13, n. 1, pp. 68-75.

- Outlaws the processing of 'sensitive' data, such as race, politics, health, religion, sexual life, or criminal record, provided proper legal safeguards are absent;
- 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[8].

Convention 108 is open for accession by non-Contracting Parties of the Council of Europe, which makes this treaty the first unified international document in data protection. Even though this Convention has numerous advantages, there is still one stumbling block. Convention 108 is binding for states that have ratified it but is not subject to the judicial supervision of the European Court of Human Rights (ECtHR).

In 1950, the Council of Europe adopted the European Convention on 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. The Convention does not presuppose the direct protection of personal data; however, Article 8 of the Convention 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. Thus, the above indicates that the Convention also covers issues of data protection in some way.

The ECtHR examined many situations involving data protection issues, such as interception of communications, sixteen various forms of surveillance by both the private and public sectors, and protection against the storage of personal data by public authorities. The ECtHR estimated that Article 8 of the Convention was one of the most violated articles in 2020 (93 cases). The right to respect for private life is not absolute since the exercise of the right to privacy

[8] DE LA TORRE, L. What is "Convention 108" [Online]. 2019 [viewed 17 January 2022]. Available from: https://medium.com/golden-data/what-is-coe-108-3708915e9846

can 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[9]. The ECtHR also established circumstances that bind the states to ensure efficient respect for private and family life.

2. Methodological Framework

The methodological basis of the research included general scientific methods, such as dialectic, system, statistic, analysis, synthesis, etc. The authors of this article also used some specific methods of international law science, including the system-legal methods, the comparative-legal methods, and the method of interpretation of the law.

The dialectical method promoted the formation of a particular general idea about personal data and their protection based on various international documents and national acts, the views of scientists who studied this issue.

The classic system method helps to make the correct order of all important documents about personal data and human rights in this sphere, to determine the relationships between them, and to provide for a special chronology of regulation. The statistical method, methods of analysis and synthesis play an important role in this study. A detailed study of the ECtHR practice makes it possible to predict the decision in a particular case and establish regularities in the proceedings and the relationship between the circumstances of the cases the court pays attention to during the proceedings. In order to improve the legal regulation of personal data protection, continuous changes in the development of legal processes and phenomena must be considered.

Numerous decisions of the ECtHR require a system-legal method to be applied. This method helps to organize the legal analysis of cases and establish important facts that influence the data protection law.

The comparative-legal method makes it possible to deduce the changes in the law on data protection from the date of the adoption of Convention 108. This method also determines the influence of digitalization on human rights. The method of legal interpretation allows the authors to study the changes in the

[9] LEVCHENKO, I., and BRITCHENKO, I. Estimation of state financial support for non-priority territorial units using the example of bridge construction. Eastern-European Journal of Enterprise Technologies, 2021, vol. 1, pp. 26-34. https://doi.org/10.15587/1729-4061.2021.225524

level of safety of human rights in the field of data protection through the paradigm of the ECtHR decisions. It is also important to mention the chronological methodology. This method determines the sequence of legal acts and court practices that regulate the protection of personal data. Thus, this method facilitates the analysis of the content of Convention 108 and numerous judgments of the ECtHR.

3. Result and Discussion

3.1. The concept of personal data through the prism of particular EU regulations

Article 8 of the European Convention on Human Rights guarantees everyone the right to respect for personal and family life, home, and correspondence. The Article also establishes that there shall be no interference by a public authority with the exercise of this right. This article does not directly cover the protection of personal data, which may be easily explained by the time of its adoption. The world has undergone a fast evolution in the technological and information spheres since 1950, which generated a need for new mechanisms for regulating human rights law. However, G. Nardell notes that the ECtHR interprets Paragraph 1 of Article 8 of the Convention quite “generously and widely.”[10] Given "modern conditions," such an interpretation allows the ECtHR to include the right to data protection in Article 8 of the Convention.

The ECHR has issued decisions on various cases about data protection during the last decades, and each of them provides a new specific interpretation of the exact problem in the sphere of personal data. In the case of S. and Marper v. the United Kingdom, the Grand Chamber of the ECtHR stressed the importance of separating and categorizing each case regarding data protection. The confirmation can be found in the following paragraph: “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

[10] NARDELL, Q.C.G. Levelling up: data privacy and the European Court of Human Rights. In: GUTWIRTH, S. POULLET, Y., and DE HERT, P. *Data Protection in a Profiled World*. Dordrecht: Springer, 2010, pp. 43-52.

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 …".[11] Thus, it is possible to conclude that the "use of personal data" has various meanings. Each kind of case requires analysis in order to determine the difference between each type of personal data and how to protect it.

In order to examine the issue of the protection of personal data, it is necessary to consider and analyze the definition of personal data first. Under the laws of the Council of Europe and the European Union (the EU), personal data is defined as information relating to an identified or identifiable natural person. 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 should consider all reasonable means to directly or indirectly identify the individual (for example, singling out). These means make 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."

Personal data can be understood as 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 and information about the public life of this person. In the case of Amann V. Switzerland, the ECtHR interpreted personal data as a notion not limited to matters of the private sphere of an individual[12]. This meaning is similar to the one provided by the General Data Protection Regulation (GDPR)[13].

[11] EUROPEAN COURT OF HUMAN RIGHTS. Case of S. and Marper v. the United Kingdom No. 30562/04 and 30566/04 [Online]. 2008 [viewed 11 March 2022]. Available from: https://rm.coe.int/168067d216

[12] EUROPEAN COURT OF HUMAN RIGHTS. Case of Amann V. Switzerland No. 27798/95 [Online]. 2000 [viewed 5 February 2022]. Available from: https://hudoc.echr.coe.int/fre#{%22fulltext%22:[%22Amann%20v.%20Switzerland%22],%22documentcollectionid2%22:[%22GRANDCHAMBER%22,%22CHAMBER%22],%22itemid%22:[%22001-58497%22]}

[13] EUROPEAN PARLIAMENT. The General Data Protection Regulation [Online]. 2016 [viewed 3 February 2022]. Available from: https://gdpr-info.eu/

The General Data Protection Regulation is the strictest privacy and security law in the world. It was adopted by the European Union in 2016. Its primary aim is to impose obligations on any organization that targets or collects 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 instruments of protection. In particular, it was an important contribution to the European data protection law when independent supervision as an instrument was included in the Directive to improve compliance with data protection rule[14].

The GDPR provides a comprehensive list of circumstances under which data processing will be possible. First of all, the permission of the subject whose data will be processed in the future must be obtained. The person must also confirm whether such processing is necessary to fulfill the terms of the contract or an assumed obligation; whether data processing is vital or aimed at protecting the interests of the individual; whether the processing is necessary for the realization of certain socially significant tasks; whether such processing is carried out within the framework of the law (except when, under such circumstances, the basic rights and freedoms of the data subject are leveled).

It is also important to mention another international act - the ePrivacy Regulation. It had to enter into force in parallel with the GDPR. The value of this document lies in the legal regulation of the use of cookies, which have become very common in recent years. After all, many sites allow us to use their services only after giving consent to the use of cookies. This is a frequent phenomenon during identity verification (for example, online shopping). According to the draft of the ePrivacy Regulation, when the user has the opportunity to either give consent or not to use the site at all, such consent cannot be considered "freely given" and therefore does not meet the requirements for consent[15]. This document is supposed to enter into force in 2023 and give companies some

[14] EUROPEAN COURT OF HUMAN RIGHTS. Guide of the European Convention on Human Rights [Online]. 2018 [viewed 5 February 2022]. Available from: https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb

[15] OSIEJEWICZ, J., ZHERLITSYN, D.M., ZADOROZHNA, S.M. OLEKSII V. TAVOLZHANSKYI and MARYNA O. DEI. National Regulation on Processing Data for Scientific Research Purposes and Biobanking Activities: Reflections on the Experience in Austria. *Asian Bioethics Review*, 2022, https://doi.org/10.1007/s41649-022-00231-4

time as a transition period. The entry into force of the ePrivacy Regulation will make it possible to improve the control over the legal relationship of personal data protection. Accordingly, this will provide more mechanisms for the adjustment of disputes and reduce them in general.

Before the GDPR, European Union had approved another regulation on personal data protection. It was the Directive of 1995. It sets up a regulatory framework that seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State set up an independent national body responsible for the supervision of any activity linked to the processing of personal data[16]. This document also proclaimed the basic right of every person – access to a due process of law. In addition, any person who has suffered damage as a result of the unlawful processing of their personal data is entitled to receive compensation for the damage suffered. The Directive provided for the principles of protection, already provided by national laws and Convention 108, and often expanded upon them.

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, regardless of the kind of personal data[17]. It is important to note that the GDPR is the instrument for regulating the data protection of EU citizens, which does not cover the entire European continent. Unlike the GDPR, ECtHR decisions are mandatory for all Member States of the Council of Europe. Thus almost countries of the European continent are part of it (except the Republic of Belarus), which makes the impact and protection of personal data much bigger.

In the context of this study, it is appropriate to examine another document, which, although is not a direct tool for personal data protection, but establishes

[16] VODOLASKOVA, K. European common aviation area: aviation liberalisation and Ukraine's accession process. *Journal of International Legal Communication*, 2021, vol. 1, n. 1, pp. 149-163. https://doi.org/10.32612/uw.27201643.2021.1.pp.149-163

[17] CHASSANG, G. The impact of the EU general data protection regulation on scientific research [Online]. 2017 [viewed 14 March 2022]. Available 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

responsibility for violation of the mechanism of processing and access to personal data. The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, was adopted with the aim of effectively countering crimes in the field of network technologies, in particular copyright infringement actions, fraud, theft of personal data. The Convention is also aimed at modernizing national legislation with the aim of countering cybercrime and, accordingly, effective prevention of such crimes.

3.2. Protection of personal data by the type of violation: the analysis of the ECtHR decisions

As mentioned previously, the ECtHR interprets the meaning of personal data according to the specific type of case. Conditionally, after years of practice, the following types of cases of data protection have been formed: interception of communications, phone tapping, and secret surveillance; monitoring of employees' computer use; voice samples; video surveillance; storage and use of personal data; disclosure of personal data; access to personal data; erasure or destruction of personal data.

Interception of communications, phone tapping, and secret surveillance are 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 and whether a fair balance was struck between the different interests involved, the European Court of Human Rights examined 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 was one of the most violated from 1978 to 2020.

The case of R.E. v. the United Kingdom is a great example of a violation of Article 8 in part of interception of communications, phone tapping, and secret surveillance. The applicant was arrested and detained in Northern Ireland on three occasions in connection with the murder of a police officer. The applicant 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 called 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 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 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 the lawyer obtained by covert surveillance[18].

However, this case is also interesting since the ECtHR established a violation and also gave an explanation why other parts of the claim were not held. According to the ECtHR decision, there had been no violation of Article 8 in part of the covert surveillance of consultations between detainees and their "appropriate adults." The Court found that detainees and their "appropriate adults" were not subject to legal privilege; 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, in so far as they related to the possible surveillance of consultations between detainees and "appropriate adults," were accompanied by adequate safeguards against abuse. Thus, as mentioned previously, the state should have a clear legal purpose to provide any type of interception of communications, phone tapping, and secret surveillance.

The next category is the monitoring of employees' computer use, which is perfectly described in the case of Barbulescu v. Romania. 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 private life and correspondence. The Grand Chamber held, by 11 votes to 6, that there

[18] EUROPEAN COURT OF HUMAN RIGHTS. Case of R.E. v. the United Kingdom No. 62498/11 [Online]. 2015 [viewed 28 January 2022]. Available from: https://www.statewatch.org/media/documents/news/2015/oct/ecxhr-judgment-full-text-R-E--v-UK-covert-surveillance-of-detainees'-consultations.pdf

had been a violation of Article 8 of the Convention. The Court found that the Romanian authorities did not protect the right to respect for private life and correspondence and failed to strike a balance between interests at stake. The national courts failed to determine whether the applicant had received prior notice from his employer of the possibility that his communications might be monitored. The national courts also did not regard that the applicant had not been informed of the nature or the extent of the monitoring or the degree of intrusion into his private life and correspondence.[19]

The ECHR also paid much attention to the issues of storage and use of personal data. In the case of S. and Marper v. the United Kingdom, the Grand Chamber said, "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 data protection under the Convention and gives the first step to understanding data protection under the practice of the ECtHR.[20]

One of the latest cases on the protection of personal data is the case of Gaughran v. the United Kingdom. This case concerned a complaint about the indefinite retention of personal data (DNA profile, fingerprints, and photograph) of a person 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

[19] EUROPEAN COURT OF HUMAN RIGHTS. Case of Barbulescu v. Romania No. 61496/08 [Online]. 2017 [viewed 18 March 2022]. Available from: https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-177082%22]}

[20] EUROPEAN COURT OF HUMAN RIGHTS. Case of S. and Marper v. the United Kingdom No. 30562/04 and 30566/04 [Online]. 2008 [viewed 11 March 2022]. Available from: https://rm.coe.int/168067d216

court underlined that the duration of the retention of data was important, and it was mandatory to pay attention to certain safeguards. The applicant's personal data had been retained indefinitely without consideration of the seriousness of the committed offense, the need for indefinite retention, or any real possibility of a review. The Court held that the retention of the applicant's data had failed to strike a fair balance between the competing public and private interests[21].

One of the categories that have a lot of cases is the disclosure of personal data. In the case of Z. v. Finland, the applicant's condition as HIV-positive in criminal proceedings was 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 the judgment of the Court of Appeal, which became available to the press, had violated the applicant's right to respect for private and family life. The ECtHR 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"[22].

It is also important to consider access to personal data through the prism of the ECtHR decisions. In the case of Turek v. Slovakia, the applicant alleged 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, it is worth noting that access to some information is possible in proceedings related to the operations of state security agencies. However, this case was related to the issue of the lustration proceeding; thus, the requirement placed an unrealistic and excessive burden on the applicant and did not respect the principle of equality. Therefore, there had 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 private life. The Court

[21] EUROPEAN COURT OF HUMAN RIGHTS. Case of Gaughran v. the United Kingdom No. 45245/15 [Online]. 2020 [viewed 8 February 2022]. Available from: https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-200817%22]}

[22] EUROPEAN COURT OF HUMAN RIGHTS. Case of Z. v. Finland No. 22009/93 [Online]. 1997 [viewed 21 March 2022]. Available from: https://www.staff.uni-mainz.de/kebert/Entscheidungen/EGMR%20Z%20v%20Finland.pdf

found it unnecessary to separately examine the effects of the applicant's registration in the former State Security Agency files and of his negative security clearance on his private life[23].

The last type of cases discussed in this article is the erasure or destruction of personal data. In the case of 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 was sentenced to a year's imprisonment in 1948 for having expressed criticism of the communist regime. The ECtHR held that there had been a violation of Article 8, stating that "… 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 that public information could fall within the scope of private life, where it was 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"[24]. 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

The European Court of Human Rights is one of the main international human rights institutions of the European system of protection of human rights, which

[23] EUROPEAN COURT OF HUMAN RIGHTS. Case of Turek v. Slovakia No. 57986/00 [Online]. 2006 [viewed 11 March 2022]. Available 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

[24] EUROPEAN COURT OF HUMAN RIGHTS. Case of Rotaru v. Romania No. 28341/95 [Online]. 2000 [viewed 17 March 2022]. Available from: http://www.hraction.org/wp-content/uploads/Rotaru_protiv_Rumunije.pdf

also provides special adjudication settlement of disputes about data protection. The European Court of Human Rights, with its decisions and recommendations, influences the formation and reformation of the contemporary national and international sphere of personal data protection. It also affects the practical use of European legal standards in making decisions by national courts. Even though 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, its rulings are not applied to the whole world. Therefore, one of the most important things is to find some general way to protect and settle disputes about personal data.

The age of the Internet and informational technologies develops so fast that more and more issues of personal data violation are arising. 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.

Considering all the issues and points about protection of personal data mentioned in this article, 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. 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

CHASSANG, G. The impact of the EU general data protection regulation on scientific research [Online]. 2017 [viewed 14 March 2022]. Available 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

DE LA TORRE, L. What is “Convention 108” [Online]. 2019 [viewed 17 January 2022]. Available from: https://medium.com/golden-data/what-is-coe-108-3708915e9846

EUROPEAN COURT OF HUMAN RIGHTS. Case of Barbulescu v. Romania No. 61496/08 [Online]. 2017 [viewed 18 March 2022]. Available from: https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-177082%22]}

EUROPEAN COURT OF HUMAN RIGHTS. Case of Gaughran v. the United Kingdom No. 45245/15 [Online]. 2020 [viewed 8 February 2022]. Available from: https://hudoc.echr.coe.int/spa#{%22itemid%22:[%22001-200817%22]}

EUROPEAN COURT OF HUMAN RIGHTS. Case of R.E. v. the United Kingdom No. 62498/11 [Online]. 2015 [viewed 28 January 2022]. Available from: https://www.statewatch.org/media/documents/news/2015/oct/ecxhr-judgment-full-text-R-E--v-UK-covert-surveillance-of-detainees'-consultations.pdf

EUROPEAN COURT OF HUMAN RIGHTS. Case of Rotaru v. Romania No. 28341/95 [Online]. 2000 [viewed 17 March 2022]. Available from: http://www.hraction.org/wp-content/uploads/Rotaru_protiv_Rumunije.pdf

EUROPEAN COURT OF HUMAN RIGHTS. Case of S. and Marper v. the United Kingdom No. 30562/04 and 30566/04 [Online]. 2008 [viewed 11 March 2022]. Available from: https://rm.coe.int/168067d216

EUROPEAN COURT OF HUMAN RIGHTS. Case of Turek v. Slovakia No. 57986/00 [Online]. 2006 [viewed 11 March 2022]. Available 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

EUROPEAN COURT OF HUMAN RIGHTS. Case of Z. v. Finland No. 22009/93 [Online]. 1997 [viewed 21 March 2022]. Available from: https://www.staff.uni-mainz.de/kebert/Entscheidungen/EGMR%20Z%20v%20Finland.pdf

EUROPEAN COURT OF HUMAN RIGHTS. Guide of the European Convention on Human Rights [Online]. 2018 [viewed 5 February 2022]. Available from: https://rm.coe.int/guide-on-article-8-of-the-european-convention-on-human-rights/16808e67cb

EUROPEAN PARLIAMENT. The General Data Protection Regulation [Online]. 2016 [viewed 3 February 2022]. Available from: https://gdpr-info.eu/

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS AND COUNCIL OF EUROPE. Handbook on European data protection law [Online]. 2018 [viewed 6 March 2022]. Available from: https://www.echr.coe.int/documents/handbook_data_protection_eng.pdf

GONZALEZ FUSTER, G. The emergence of personal data protection as a fundamental right of the EU. Cham: Springer, 2016.

KOMKOVA, G. N., BASOVA A. V., and TOROSYAN R. A. Constitutional protection of public figures' personal data on the Internet. *Journal of Siberian Federal University. Humanities & Social Science*, 2020, vol. 13, n. 1, pp. 68-75.

LEVCHENKO, I., and BRITCHENKO, I. Estimation of state financial support for non-priority territorial units using the example of bridge construction. Eastern-European Journal of Enterprise Technologies, 2021, vol. 1, pp. 26-34. https://doi.org/10.15587/1729-4061.2021.225524

NARDELL, Q.C.G. Levelling up: data privacy and the European Court of Human Rights. In: GUTWIRTH, S. POULLET, Y., and DE HERT, P. *Data Protection in a Profiled World*. Dordrecht: Springer, 2010, pp. 43-52.

OGANESIAN, T. D. The right to privacy and data protection in the information age. *Journal of Siberian Federal University. Humanities & Social Science*, 2020, vol. 13, n. 10, pp. 1576-1588.

OSIEJEWICZ, J., ZHERLITSYN, D.M., ZADOROZHNA, S.M. OLEKSII V. TAVOLZHANSKYI and MARYNA O. DEI. National Regulation on Processing Data for Scientific Research Purposes and Biobanking Activities: Reflections on the Experience in Austria. *Asian Bioethics Review*, 2022, https://doi.org/10.1007/s41649-022-00231-4

VODOLASKOVA, K. European common aviation area: aviation liberalisation and Ukraine's accession process. *Journal of International Legal Communication*, 2021, vol. 1, n. 1, pp. 149-163. https://doi.org/10.32612/uw.27201643.2021.1.pp.149-163

Data de submissão do artigo:26/09/2022

Data de aprovação do artigo: 27/02/2023

Edição e propriedade:

Universidade Portucalense Cooperativa de Ensino Superior, CRL

Rua Dr. António Bernardino de Almeida, 541 - 4200-072 Porto

Email: upt@upt.pt