

**XXI међународни научни скуп „Правнички дани –
Проф. др Славко Царић“
„ОДГОВОРИ ПРАВНЕ НАУКЕ НА ИЗАЗОВЕ САВРЕМЕНОГ
ДРУШТВА“**

**XXI International Scientific Conference „Legal days –
Prof. Slavko Carić, PhD“
"THE RESPONSES OF LEGAL SCIENCES TO THE CHALLENGES OF
MODERN SOCIETY"**

Универзитет Привредна академија у Новом Саду
Правни факултет за привреду и правосуђе у Новом Саду
The University of Business Academy in Novi Sad
The Faculty of Law for Commerce and Judiciary in Novi Sad

Нови Сад, 04. и 05. октобар 2024.

Зборник радова са XXI међународног научног скупа
„Правнички дани – Проф. др Славко Царић“

„ОДГОВОРИ ПРАВНЕ НАУКЕ НА ИЗАЗОВЕ САВРЕМЕНОГ ДРУШТВА“

04. и 05. октобар 2024. године у Новом Саду,
у организацији Универзитета Привредна академија у Новом Саду
Правни факултет за привреду и правосуђе у Новом Саду

Издавач:

Универзитет Привредна академија у Новом Саду
Правни факултет за привреду и правосуђе у Новом Саду
Гери Кароља бр. 1, телефон: 021/ 400 - 499
Web: www.pravni-fakultet.info

Рецензенти:

Др Милан Почуча редовни професор	Др Сања Шкорић ванредни професор
Др Владимир Козар редовни професор	Др Јоко Драгојловић ванредни професор
Др Јелана Матијашевић редовни професор	Др Маријана Младенов ванредни професор
Др Милош Марковић редовни професор	Др Ненад Бингулац ванредни професор
Др Предраг Мирковић редовни професор	Др Марко Станковић ванредни професор
Др Дарко Голић редовни професор	Др Далибор Крстинић ванредни професор
Др Јелена Шогоров Вучковић редовни професор	Др Ненад Стефановић ванредни професор
	Др Дејан Логарушић ванредни професор

За издавача:

Др Милан Почуча, редовни професор

Уредник:

Др Милан Почуча, редовни професор

Штампа:

Граф 021, Нови Сад

Тираж: 150

ISBN 978-86-86121-64-6

Научни одбор:

ПРОФ. ДР МИЛАН ПОЧУЧА - председник Научног одбора

Декан Правног факултета за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МАРКО ЦАРИЋ

Декан Факултета за економију и инжењерски менаџмент, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МАРИЈАНА ЦАРИЋ

Председник Савета Универзитета Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МИРКО КУЛИЋ

Професор емеритус на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МАРИЈАНА ДУКИЋ МИЈАТОВИЋ

Редовни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ПРЕДРАГ МИРКОВИЋ

Председник Савета Правног факултета за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР МАРИЈАНА МЛАДЕНОВ

Продекан за међународну сарадњу на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ЗОРАН ПАВЛОВИЋ

Шеф Кривичноправне катедре на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ДАРКО ГОЛИЋ

Шеф Теоријске и јавноправне катедре на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ЖЕЉКО БЈЕЛАЈАЦ

Редовни професор на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ЈЕЛЕНА МАТИЈАШЕВИЋ

Продекан за науку на Правном факултету за привреду и правосуђе, Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ВЛАДИМИР КОЗАР

Редовни професор на Правном факултету за привреду и правосуђе,
Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР САЊА ШКОРИЋ

Продекан за наставу на Правном факултету за привреду и правосуђе,
Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ЈОКО ДРАГОЈЛОВИЋ

Ванредни професор на Правном факултету за привреду и правосуђе,
Универзитет Привредна академија у Новом Саду | Република Србија

ПРОФ. ДР ВЛАДИМИР ЦАТИЕВ

Шеф катедре Кривичноправних наука Руске академије за адвокатуру и
нотаријат | Руска Федерација

ПРОФ. ДР БРАНКО ВУЧКОВИЋ

Председник Удружења за кривично право и криминалну политику Црне Горе
| Република Црна Гора

ПРОФ. ДР ВЕСНА ВУЧКОВИЋ

Судија Врховног суда Црне Горе | Република Црна Гора

PROF. DR DR. WOLFGANG ROHRBACH

Akademik Evropske akademije nauka u Salzburgu | Austrija

PROF. DR. AMER FAKHOURY

Dean College of Law American University in the Emirates | Ujedinjeni Arapski
Emirati

ДОЦ. ДР БРАНИСЛАВ ДУДИЋ

Доцент на Факултету за менаџмент, Универзитет Коменски Братислава
| Република Словачка

ПРОФ. ДР ЗОРАН ФИЛИПОВСКИ

Проректор за међународну сарадњу, Интернационални „Vision”
Универзитет | Северна Македонија

PROF DR KONSTANTINOS KOUROUPIS

University Frederik | Kipar

DR VIKTÓRIA CSIZMADIÁNÉ CZUPPON

Viši naučni saradnik, Poslovno-ekonomski fakultet, Univerzitet u Panoniji
| Mađarska

DOC. DR. SC. SANJA GONGETA, PROF. STRUČ. STUD.

Prodekanica za stručni naučnoistraživački rad i međunarodnu saradnju
Veleučilište Lavoslav Ružička u Vukovaru | Republika Hrvatska

PROF DR CRISTINA ELENA POPA TACHE

Fakultet za psihologiju, bihejvioralne i pravne nauke, Univerzitet "Andrei Sagun",
Akademija za ekonomske studije u Bukureštu | Rumunija

PROF DR ADELA DANAJ

Viši predavač na Političkim naukama i međunarodnim odnosima, Predsedavajući
Centra za istraživanje, projekte i inovacije, Univerzitet Njujork u Tirani | Albanija

PROF. DR VALENTINA RANALDI

Pravni fakultet, Univerzitet "Niccolò Cusano" | Italija

ПРОФ. ДР НЕБОЈША ШАРКИЋ

Професор емеритус Правног факултета, Универзитета Унион у Београду
| Република Србија

ПРОФ. ДР ВЛАДИМИР ЧЛОВИЋ

Директор Института за упоредно право у Београду | Република Србија

ПРОФ. ДР МИЛОШ МАРКОВИЋ

Редовни професор на Правном факултету за привреду и правосуђе,
Универзитет Привредна академија у Новом Саду | Република Србија

Организациони одбор:

ПРОФ. ДР ЈОКО ДРАГОЈЛОВИЋ - ПРЕДСЕДНИК ОРГАНИЗАЦИОНОГ ОДБОРА

ПРОФ. ДР ИВАН ЈОКСИЋ

ПРОФ. ДР ЈЕЛЕНА СТОЈШИЋ ДАБЕТИЋ

ПРОФ. ДР НЕНАД БИНГУЛАЦ

ПРОФ. ДР НЕНАД СТЕФАНОВИЋ

ПРОФ. ДР МАРКО СТАНКОВИЋ

ПРОФ. ДР ДАЛИБОР КРСТИНИЋ

ДОЦ. ДР МАЈА ПЕТРОВИЋ

ДР ИСИДОРА МИЛОШЕВИЋ

МСР АЊА КОПРИВИЦА

МР МАРА ДЕСПОТОВ

МСР ТАМАРА КРСТИЋ

Секретар:

МСР АЊА КОПРИВИЦА, асистент

UDC: 342:738:004(4)
DOI: 10.5937/PDSC24371S

Tamara Staparski, MA in Criminalistics

*Teaching Assistant, Faculty of Law for Commerce and Judiciary in Novi Sad,
Republic of Serbia*

email: tamara.staparski@pravni-fakultet.info

Valentina Ranaldi, PhD, Associate Professor

“Niccolò Cusano” University of Rome, Italy

email: valentina.ranaldi@unicusano.it

COUNCIL OF EUROPE APPROACH TOWARDS THE RIGHT TO PRIVACY IN DIGITAL DOMAIN: RECENT DEVELOPMENT*

Abstract:

Modern technology is an essential component of modern life, and there is a strong connection between our physical reality and our digital world. Communication is a fundamental attribute of individuals and an integral aspect of social interaction, employment, and overall existence. In today's society, communication through social networks, emails, and Instant Messaging applications (IM) is an integral part of a modern individual's daily life. The IMs are the most accessible, widely used, and cost-effective means of transmitting and receiving information. Since that information reveals and contains a great part of our privacy, employing it makes us vulnerable and exposed to privacy violations. To protect user privacy, IMs (like other means of electronic communication) use encryption to safeguard sensitive data exchanged and transmitted between users. This defines the subject of the research in the paper referring to the right to privacy and right to private communication in the digital domain, from the perspective of the Council of Europe according to Article 8 of the European Convention on Human Rights and Article 11 of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. The special attention will be devoted to the *Podchasov v. Russia* case which concerns the right to privacy by protecting the encryption of sensitive data of electronic communications via IMs Telegram in the Russian Federation. In

*Paragraphs 1, 3 and 4 are by Tamara Staparski; paragraphs 2 and 5 are by Valentina Ranaldi.

concluding remarks, the authors highlight the significance of the *Podchasov v. Russia* case and the Council of Europe Framework Convention as a starting point for future action and the establishment of new standards in this field.

Keywords: *the right to privacy, AI, digital domain, ECtHR, Council of Europe*

1. Introduction

"Once you've lost your privacy, you realize you've lost an extremely valuable thing."¹

Since its inception, the human race has been striving to improve and involve constantly. Every civilisation through its distinguished individuals spawned discoveries to enhance the quality of everyday life, leaving, at the same time, an indelible mark in human history. From a steam engine, electricity, light bulb and electric batteries, through the first telephone, aeroplane, and computer to modern technological gates and artificial intelligence (AI), we unconsciously have turned our desire for progress into our greatest weakness. Since a significant part of our lives has gradually but insidiously moved into the digital domain, we naively concluded that life is much easier on the screen. Fake friends, fabricated lives, spurious happiness and one real thing- our privacy given to the world on a golden platter. But what about those who are desperate to preserve their privacy and keep it to themselves? Does privacy preservation mean disconnection from the digital world? If so, can we “exist” in modern times if we are not “connected” and do we have to choose between protection of our private life and a sense of belonging to the herd that keeps pace with time? Unquestionably, AI-powered systems play a major role in making daily life easier, reflected in the fight against climate change and biodiversity preservation, as well as in the advancement of living standards, transportation, industrial and medical innovations, and communication systems.² However, as these AI systems develop more rapidly and without adequate legal oversight, human rights and freedoms are exposed to greater risk, especially through uncontrolled collection and processing of personal data.

So, for man to live and behave in harmony with rapid technological development, it is necessary to establish legal rules and limits on the impact of technological innovations on human rights and man's everyday life. A free and

¹ Billy Graham, in A-Z Quotes | Quotes for All Occasions (azquotes.com), (6 July, 2024). Retrieved from: https://www.brainyquote.com/quotes/billy_graham_446542

² Leslie, D., Burr, C., Aitken, M., Cows, J., Katell, M., and Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe, p. 5.

democratic society cannot exist without the fundamental human right to privacy.³ Being a valuable part of each individual's personality, it enables us to be sheltered from harmful external influences and stay nestled within our universe. Since Convention for the Protection of Human Rights and Fundamental Freedoms⁴ in Article 8 established the right for respect of the private and family life, home and correspondence⁵, the question arises whether our privacy – especially the privacy of our correspondence- has the same importance and protection online and offline.

2. The right to privacy in the digital domain

Privacy- a short but powerful word. Nowadays, often taken for granted, undervalued and highly mistreated. The conceptualizations of privacy have evolved with technology evolution, moving from a "right to be left alone" to a more complex dimension in different spheres of social relations in which technology is deeply incorporated, such as legal, political, social and economic aspects of the society.⁶

With the exponential growth of internet-based activities, privacy has become a popular phrase in the information age.⁷ While a specific definition for the term "privacy" is lacking, it can be defined as an individual's right to a certain amount of control over the collection and use of personal data.⁸ But, what is a “certain amount” and are we able to decide in any case to what extent, in what way and by whom our data will be collected and processed? And if so, can we be sure that in certain situations our data, especially our privacy will be protected if violated? Various programs and apps we use daily, such as Google, Instagram, Facebook, Amazon, Twitter, WhatsApp, Viber, etc. collect and process our personal data, putting our privacy in question. Taking into account that the varieties of apps are so wide and that they can satisfy the needs of all possible and impossible aspects of use, as well as the tempting fact that the use of a large number of apps is free of charge, the consequence of these benefits is "adequate compensation" by the user. When installing, the majority of apps on the Play Store request authorisation to use our device's microphone, camera, contacts, location, and other features. This entails having access to our sensitive information, such as our voice and speech, location,

³ Gilani, S. R. S., Al-Matrooshi, A. M., & Khan, M. H. (2023). Right of Privacy and the Growing Scope of Artificial Intelligence. *Current Trends in Law and Society*, 3(1), p. 2.

⁴ Convention for the Protection of Human Rights and Fundamental Freedoms (1950), Council of Europe, Europe Treaty Series No. 005

⁵ Ibid, p. 4-5.

⁶ Friedewald, M. and Finn, R. and Wright, D. (2013). European Data Protection: Coming of Age. Chapter: Seven Types of Privacy. Springer Science+Business Media Dordrecht, p. 1.

⁷ Tiwari, M., and Pandey, A. K., (2021). Socio-legal Impact on Privacy in AI-Driven World. *IOSR Journal of Humanities And Social Science (IOSR-JHSS)*, Volume 26, Issue 4, Series 3, p. 39.

⁸ Gulati, T. op. cit., p. 23.

etc. If a sizable portion of the apps requiring these permissions do not even suggest that access to these data is necessary for the app to work properly, then the issue may not seem quite so absurd. Granting permissions is voluntary and necessary for each area of our privacy independently, but surprisingly, most apps will not work properly or at all, if all permissions are not granted. So it may seem that the currency of being part of a modern society that cannot function without the digital world is more expensive than we could ever imagine – instead of money, we pay with our privacy. We cannot, however, entirely place the responsibility on the developers of programs and apps of which we have become passionate users and rely so heavily on. For example, social network users seem to deliberately overlook the fact that when they upload material, they often give the platform operator copyright, yet they share extremely private information with impunity.⁹ Therefore, the question arises: If we do not protect and value our privacy, is it legitimate to expect someone else to do so? In light of this, the authors believe that users' ignorance, the various ways that digital technology developers gather personal data about them, and the fact that people typically take their privacy for granted without considering the repercussions, call for more attention to be paid to privacy in the digital domain.

The right to privacy is a particular human right, given how human rights are established. Considering that human rights originated within nation-states and were subsequently elevated to the international level once the concept had sufficiently developed, it is intriguing to note that this progression did not occur with the right to privacy.¹⁰ The origins of the protection of human rights can be traced back to the laws of ancient Babylon, but the advancement of human rights as they are known today gained momentum following the conclusion of World War II.¹¹ At that time, no constitution included a comprehensive provision guaranteeing the right to privacy and the recognition of the "right to privacy" as a fundamental human right, occurred at the international level before its formal proclamation in any constitution.¹² Today, every human has the fundamental right to privacy, outlined in numerous treaties. Following Article 12 of the Universal Declaration of Human Rights¹³, the Council of Europe has recognised the necessity for the protection of privacy, articulated in Article 8 of ECHR stating everyone's „right to respect for his private and family life,

⁹ Gulati, T. (2022). Artificial Intelligence and privacy violation. *Journal of Unique Laws and Students-* Vol. 2 Issue II, p. 24.

¹⁰ Diggelmann, O., and Cleis, M. N., (2014). How the Right to Privacy Became a Human Right. *Human Rights Law Review*, Volume 14, Issue 3, pp. 441-442.

¹¹ Salkesh. R. Kori., (2018). Historical Development of Human Rights. *International Journal of Research in all Subjects in Multi Languages*, Vol. 6, Issue: 9, pp. 2-5.

¹² Diggelmann, O., and Cleis, M. N., op. cit., pp. 441-442.

¹³ Universal Declaration of Human Rights (1948), United Nations, 217 A (III), p. 4.

his home and his correspondence“, with the potential to restrict this right under the conditions outlined in the Convention.¹⁴

However, when the ECHR was adopted (1950)¹⁵, the Internet¹⁶, which is now an indispensable part of our lives, was not even considered or anticipated. Since even the Protocols that changed the framework of the Convention did not address the issue of the right to privacy in the digital domain or any other proclaimed human right, especially taking into account the growing influence of AI, the Council of Europe adopted in Strasbourg on May 17, 2024, the “first-ever international legally binding treaty aimed at ensuring the respect of human rights, the rule of law and democracy legal standards in the use of artificial intelligence (AI) systems”.¹⁷

3. Right to privacy from the perspective of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law

Defining the term AI is very complex and cannot be determined from the point of view of a single science. The term "artificial intelligence" was first used by John McCarthy¹⁸ in 1956, meaning a computer's capacity for learning that allows it to perform increasingly challenging tasks, such as translating, playing chess, and recognizing language and images.¹⁹ The idea of comprehending AI evolved along with society and technology. Nevertheless, despite varying interpretations of the term, AI has undeniably been ingrained in our daily lives and has spread to every aspect of our existence. Using AI-based systems, especially in the social sphere, makes us vulnerable, exposing our private lives to the public eye.

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law is adopted as a response to the accelerated technological development, particularly the changes brought about by the life cycle activities of AI systems, which enable the prosperity of society and human

¹⁴ European Convention on Human Rights, op. cit. Article 8.

¹⁵ The European Convention on Human Rights, in Council of Europe (26 July, 2024). Retrieved from: <https://www.coe.int/en/web/human-rights-convention>

¹⁶ The inception of the Internet may be traced back to the year 1960. See more at: <https://en.wikipedia.org/wiki/Internet>

¹⁷ Newsroom, in Council of Europe (26 July, 2024). Retrieved from: <https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence>

¹⁸ John McCarthy was an American computer scientist and cognitive scientist, and one of the founders of the discipline of artificial intelligence (14 July, 2024). Retrieved from: [https://en.wikipedia.org/wiki/John_McCarthy_\(computer_scientist\)](https://en.wikipedia.org/wiki/John_McCarthy_(computer_scientist))

¹⁹ Angjeli, G. and Premalaj B. (2021). Human Rights - From reality to the virtual world. The right to respect private life in the context of the development of artificial intelligence. House WSGE Alcide De Gasperi University of Euroregional Economy, p. 11.

rights, but at the same time discriminate and cause inequality in the digital context, undermine human rights, the autonomy of individuals, human dignity, democracy and the rule of law.²⁰

As for the right to privacy, Article 11 which is dedicated to privacy and personal data protection, proclaims that:

“Each Party shall adopt or maintain measures to ensure that, with regard to activities within the lifecycle of artificial intelligence systems:

a privacy rights of individuals and their personal data are protected, including through applicable domestic and international laws, standards and frameworks; and

b effective guarantees and safeguards have been put in place for individuals, in accordance with applicable domestic and international legal obligations.”²¹

The authors find this provision too general, as it fails to address the issue of discretionary evaluation of the extent to which the right to privacy is protected, as well as the question of what constitutes adequate effective safeguards and protective measures. This is particularly concerning given the rapid advancement of information technologies and AI, and the inability of legal systems, both national and international levels, to keep pace with this progress. However, according to the Convention, every party must establish an autonomous system for monitoring and regulating compliance with the Convention, and increase the understanding and general knowledge of the public about the appropriate use of AI-based systems, about which proper information will be acquired through different suitable sources.²²

The Framework Convention will be available for signing in Vilnius, Lithuania, on September 5, 2024, during the Conference of Ministers of Justice.²³ Nevertheless, the practical effectiveness of the Convention, the acts of parties in compliance with the defined requirements outlined in the Convention, and the European Court of Human Rights (ECtHR) approach in determining violations of Convention provisions is yet to be seen in practice. Until then, Article 8 of the ECHR remains a strong foundation for protecting the right to privacy, both offline and potentially online as well, as demonstrated by the ruling of the ECtHR in the case *Podchasov v. Russia*²⁴.

²⁰ Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024), Council of Europe Treaty Series - No. [225], p. 1.

²¹ Ibid, p. 5.

²² Newsroom, in Council of Europe, op. cit.

²³ Ibid.

²⁴ *Anton Valeryevich Podchasov v. Russian Federation*, Application no. 33696/19, Decission ECtHR February 13, 2024.

4. The case of *Podchasov v. Russia*

In today's society, communication through social networks, emails, and Instant Messaging applications (IM) is an integral part of a modern individual's daily life. The IMs are the most accessible, widely used, and cost-effective means of transmitting and receiving information. Since that information reveals and contains a great part of our privacy, employing it makes us vulnerable and exposed to privacy violations. To protect user privacy, IMs (like other means of electronic communication) use encryption to safeguard sensitive data exchanged and transmitted between users. As encryption refers to a process of transforming plaintext messages into incomprehensible code that can only be decoded (decrypted) by someone possessing the confidential key²⁵, the choice of encryption method will directly impact the level of security for data protection. The most common encryption used by IMs is end-to-end encryption (E2EE)²⁶. By employing encryption techniques, sensitive personal information is protected from unauthorised access, which is achieved by encoding the data to allow only the intended recipients to decrypt and access the content using either public or private keys.²⁷

The *Podchasov v. Russia* case concerns the right to respect private life and the privacy of communications carried out through the Telegram messaging application. Under Russian law, "internet communication organisers" (ICO) are required to retain all communication data (metadata) for one year and the content of communications for six months. This also includes the obligation of providing the data and necessary decryption "keys" to competent authorities upon request, as specified by law. These data are obtained from a wide range of electronic communications commonly used by Internet users worldwide. Mr Anton Valeryevich Podchasov, a Russian citizen, was using the Telegram Messenger LLP when he submitted his application to the ECtHR in 2019. In July 2017, the Russian Federal Security Service made a formal request to Telegram for sensitive information regarding six individuals, including the applicant, who were suspected of engaging in terrorist activities. This information included the necessary data associated with the keys to decode the correspondence between suspects carried out through the Telegram platform. However, Telegram responded to the request by stating that the individuals in question were

²⁵ Endeley, R. E., (2018). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. *Journal of Information Security*, Vol. 9, p. 96.

²⁶ Ilmonen, M., (2020). Platform-Agnostic End-to-End Encryption for Modern Instant Messaging Platforms. University of Aberdeen, p. 10.

²⁷ Dissanayaka, R. et. al., (2023). Review paper on the End-to-End encryption technique used in Social media applications, in Research Gate, p. 1. Retrieved from: https://www.researchgate.net/publication/375999294_Review_paper_on_the_End-to-End_encryption_technique_used_in_Social_media_applications

communicating through a „secret chat“, which utilizes end-to-end (client- client) encryption. Consequently, the chat is inherently inaccessible to anybody other than the participants, including Telegram, unless a backdoor is created, which would compromise the encryption system for all users, so Telegram declined to comply with the request. As a result, Russian courts decisions imposed fines on Telegram and mandated the blocking of the Telegram app in Russia.

In March 2018, the applicant and 34 other users disputed the request issued to Telegram by the Federal Security Service. The complaint highlighted that if the Federal Security Service were to acquire the encryption keys, they would possess the technical capability to decrypt and access the communications of all Telegram users without requiring a court order, as mandated by the current legislation in Russia, which would breach their right to respect private life and privacy of communications. However, the complaint was rejected as inadmissible since no violation of the plaintiff's rights was established, and notwithstanding the court decision prohibiting Telegram, it remains operational in Russia. After exhausting all available legal remedies in Russia, on June 18, 2019, Mr Anton Valeryevich Podchasov filed an application to the ECtHR against the Russian Federation for violation of Article 8 of the ECHR. As disputed, he emphasized the legal obligation for the ICOs to retain and provide any electronic communications and associated data upon request from competent authorities, including decryption data for encrypted communications.

Following the proceedings, the ECtHR, among other matters, concluded that it has the authority to review the current application about the events that led to the reported violations of the Convention that took place before 16 September 2022, which is the date when the Russian Federation withdrew from the Convention. In addition, the ECtHR determined that the applicant's rights under Article 8 of the Convention are being interfered with by Telegram's legal obligation to continuously store the applicant's electronic communications and related data, as well as to grant authorities access to this data and require Telegram to decrypt encrypted data. Moreover, the ECtHR emphasized that individuals using electronic communications and the Internet should be ensured that their privacy and freedom of speech be upheld. However, this assurance is not absolute, but rather restricted to the objectives outlined in Article 8 of the Convention.

Due to the fact that the rise in Internet usage and digital communication has led to a significant increase in the risk of different forms of abuse for signature countries and Internet users, the ECtHR acknowledged that the challenged legal provisions in Russia, which aim to safeguard national security, prevent disorder and crime, and protect the rights and freedoms of individuals, are legitimate. However, the ECtHR found that the contested law lacks adequate safeguards to prevent abuses

related to access to electronic communications data, which ICOs have a legal duty to protect.

Furthermore, the ECtHR highlighted that the delivery of necessary data to authorized entities for decrypting encrypted electronic communications is crucial in preventing illegal access to the content of communications. This is directly linked to the protection of the right to respect for private life and privacy of correspondence on the Internet.

Based on all established facts, the ECtHR, unanimously, concluded that it is inadmissible for the contested legislation—which requires that all Internet communications be retained, that security services have direct access to data that is stored without sufficient safeguards against abuse, and that end-to-end encrypted communications require that all communications be decrypted—to be considered necessary in a democratic society. This legislation violates the fundamental right to privacy, as outlined in Article 8 of the ECHR, by allowing public authorities to access electronic communications without adequate safeguards. Therefore, the respondent State has exceeded the permissible level of discretion in this matter and the ECtHR concluded that Article 8 of the ECHR has been breached.²⁸

5. Conclusion

Undoubtedly, we live in an era where technology advances at a faster pace than we do, and we, paradoxically, somehow try to keep up with it; in an era in which our lives move swiftly rather than progressing gradually, and we, obsessed with technology, are oblivious to it; in an era when we easily give up our privacy or, on the other hand, frantically try to keep it for ourselves as it gives us freedom or at least the feeling of it; in an era when the law is falling behind in the battle against time, while technology rapidly advancing towards its objectives. Given our dependence on the Internet and the constant use of social networks and IMs, it is imperative to prioritize the protection of privacy in the digital domain, especially considering the significant threats it faces. This objective can be accomplished by a dual approach: first, by providing users with education and increasing their awareness about the need to safeguard their privacy and keep sensitive information confidential; and second, by adopting appropriate legal frameworks to safeguard the right to privacy in the digital domain. The ECtHR's judgment in the case *Podchasov v. Russia* holds immense importance in safeguarding data encryption on the Internet since it has become a modern-day imperative for reliable data exchange. The authors believe that this judgment will be adopted as a standard procedure in court hearings involving

²⁸ Anton Valeryevich Podchasov v. Russian Federation, op. cit. p. 23.

comparable circumstances. Additionally, the authors expect it to serve as a commendable model and reference for future court proceedings in other jurisdictions. By adopting the Framework Convention on artificial intelligence and human rights, democracy, and the rule of law, the Council of Europe indicated the necessity of regulating human rights in the digital world, which are becoming seriously threatened by the rapid development of AI. Given that the convention will be available for signatures starting on September 5, 2024, the authors consider its approval to be a significant milestone and the first stage in the establishment of standards in this field.

Tamara Staparski, mast. krim

*Asistent na Pravnom fakultetu za privredu i pravosuđe u Novom Sadu,
Univerzitet Privredna akademija u Novom Sadu*

Dr Valentina Ranaldi, vanredni profesor

na "Nikolo Kuzano" univerzitetu u Rimu, Italija

PRISTUP SAVETA EVROPE PRAVU NA PRIVATNOST U DIGITALNOM DOMENU: NEDAVNA DOSTIGNUĆA

Apstrakt:

Moderna tehnologija je esencijalni deo savremenog života i postoji snažna veza između našeg fizičke realnosti i našeg digitalnog sveta. Komunikacija je osnovni atribut pojedinaca i integralni aspekt društvene interakcije, rada i celokupnog postojanja. U današnjem društvu, komunikacija putem društvenih mreža, mejlova i aplikacija za razmenu instant poruka (IM) sastavni je deo svakodnevnog života svakog pojedinca. IM su najpristupačnije, u širokoj upotrebi i najjeftinije sredstvo za prenos i prijem informacija. Budući da te informacije otkrivaju i sadrže veliki deo naše privatnosti, njihova upotreba nas čini ranjivim i izloženim zloupotrebi privatnosti. Da bi zaštitile privatnost korisnika, IM (kao i druga sredstva elektronske komunikacije) koriste šifrovanje kako bi zaštitili osetljive podatke koji se razmenjuju i prenose između korisnika. Ovo predstavlja predmet istraživanja u radu koji se odnosi na pravo na privatnost i pravo na privatnu komunikaciju u digitalnom domenu iz perspektive Saveta Evrope kroz član 8 Evropske konvencije o ljudskim pravima i član 11 Okvirne konvencije Saveta Evrope o veštačkoj inteligenciji i ljudskim pravima, demokratiji i vladavini prava. Posebna pažnja biće posvećena analizi slučaja *Podčasov protiv Rusije* koji se tiče zaštite prava na privatnost zaštitom šifrovanja osetljivih podataka elektronskih komunikacija putem IM Telegram u Ruskoj Federaciji. U zaključnim napomenama, autori ističu značaj predmeta *Podčasov protiv Rusije* i Okvirne konvencije Saveta Evrope o veštačkoj inteligenciji i ljudskim

pravima, demokratiji i vladavini prava, kao polazne tačke za buduće postupanje i uspostavljanje novih standarda u ovoj oblasti.

***Ključne reči:** pravo na privatnost, AI, digitalni domen, Evropski sud za ljudska prava, Savet Evrope*

References:

1. Angjeli, G. and Premalaj B. (2021). Human Rights - From reality to the virtual world. The right to respect private life in the context of the development of artificial intelligence. House WSGE Alcide De Gasperi University of Euroregional Economy ul. Sienkiewicza 4 05-410 Józefów, pp. 10-19. DOI: 10.13166/WSGE//VPTV1229
2. Billy Graham, in A-Z Quotes | Quotes for All Occasions (azquotes.com), (6 July, 2024). Retrieved from:
https://www.brainyquote.com/quotes/billy_graham_446542
3. Convention for the Protection of Human Rights and Fundamental Freedoms (1950), Council of Europe, Europe Treaty Series 005, pp. 1-62.
4. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024), Council of Europe Treaty Series - No. [225], pp. 1-12.
5. Diggelmann, O., and Cleis, M. N., (2014). How the Right to Privacy Became a Human Right. Human Rights Law Review, Volume 14, Issue 3, pp. 441-458.
6. Dissanayaka, R. et. al., (2023). Review paper on the End-to-End encryption technique used in Social media applications, in Research Gate, pp. 1-4. Retrieved from:
https://www.researchgate.net/publication/375999294_Review_paper_on_the_End-to-End_encryption_technique_used_in_Social_media_applications
7. Endeley, R. E., (2018). End-to-End Encryption in Messaging Services and National Security—Case of WhatsApp Messenger. Journal of Information Security, Vol. 9, pp. 95-99.
8. Friedewald, M. and Finn, R. and Wright, D. (2013). European Data Protection: Coming of Age. Chapter: Seven Types of Privacy. Springer Science+Business Media Dordrecht, p. 1. / S. Gutwirth et al. (eds.), European Data Protection: Coming of Age, DOI 10.1007/978-94-007-5170-5_1, © Springer Science+Business Media Dordrecht 2013, pp. 3-27
9. Gilani, S. R. S., Al-Matrooshi, A. M., & Khan, M. H. (2023). Right of Privacy and the Growing Scope of Artificial Intelligence. Current Trends in Law and Society, 3(1), 1–11. <https://doi.org/10.52131/clts.2023.0301.0011>

10. Gulati, T. (2022). Artificial Intelligence and privacy violation. *Journal of Unique Laws and Students-* Vol. 2 Issue II, pp. 22-31.
11. Ilmonen, M., (2020). Platform-Agnostic End-to-End Encryption for Modern Instant Messaging Platforms. University of Aberdeen, pp. 1-76.
12. Internet, in Wikipedia (26 July, 2024). Retrieved from:
<https://en.wikipedia.org/wiki/Internet>
13. John McCarthy, on Wikipedia (14 July, 2024). Retrieved from:
[https://en.wikipedia.org/wiki/John_McCarthy_\(computer_scientist\)](https://en.wikipedia.org/wiki/John_McCarthy_(computer_scientist))
14. Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., and Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: a primer. The Council of Europe, pp. 1-46.
15. Newsroom, in Council of Europe (26 July, 2024). Retrieved from:
<https://www.coe.int/en/web/portal/-/council-of-europe-adopts-first-international-treaty-on-artificial-intelligence>
16. Salkesh. R. Kori., (2018). Historical Development of Human Rights. *International Journal of Research in all Subjects in Multi Languages*, Vol. 6, Issue: 9, pp. 2-8.
17. Tiwari, M., and Pandey, A. K., (2021). Socio-legal Impact on Privacy in AI-Driven World. *IOSR Journal of Humanities And Social Science (IOSR-JHSS)*, Volume 26, Issue 4, Series 3, pp. 39-48
18. Universal Declaration of Human Rights (1948), United Nations, 217 A (III), pp. 2-8.

CIP - Каталогизација у публикацији Библиотека Матице српске, Нови Сад

34:316.3"20"(082)

МЕЂУНАРОДНИ научни скуп "Правнички дани - проф. др Славко Царић" (21 ; 2024 ; Нови Сад)

XXI међународни научни скуп "Правнички дани - Проф. др Славко Царић" "Одговори правне науке на изазове савременог друштва", Нови Сад, 4. и 5. окт. 2024 = XXI International Scientific Conference "Legal days - Prof. Slavko Carić, PhD" "The Responses of Legal Sciences to the Challenges of Modern Society" : [зборник радова] / [уредник Милан Почуча]. - Нови Сад : Универзитет Привредна академија, Правни факултет за привреду и правосуђе, 2024 (Нови Сад : Граф 021). - 770 стр. : илустр. ; 24 cm

Радови на срп. (ћир. и лат.) и енгл. језику. - Тираж 150. - Стр. 23-26: Уводна реч / Милан Почуча = Opening word / Milan Počuča. - Напомене и библиографске референце уз текст. - Библиографија уз сваки рад. - Резиме на енгл. језику уз сваки рад.

ISBN 978-86-86121-64-6

а) Правна наука - Савремено друштво - 21. в. – Зборници

COBISS.SR-ID 153244169