eudaimonia

Revija za pravnu, političku i socijalnu teoriju i filozofiju

Journal for Legal, Political and Social Theory and Philosophy

Vol. 8 No. 1 • 2024.

Izdavač

IVR Srbija

Srpsko udruženje za pravnu i socijalnu filozofiju

Izdavač:

Centar za temeljna pravna znanja,
Srpsko udruženje za pravnu i socijalnu filozofiju (IVR Srbija),
Pravni fakultet Univerziteta u Beogradu

Glavni i odgovorni urednik:

dr Julieta Rabanos
(Univerzitet u Beogradu – Pravni fakultet)

Izvršni urednici:

Ana Zdravković
(Univerzitet u Beogradu – Pravni fakultet)
Mila Đorđević
(Univerzitet u Beogradu – Pravni fakultet)

Studentska redakcija:

Petar Mitrović (Univerzitet u Beogradu – Pravni fakultet), Fani Spalević (Univerzitet u Beogradu – Pravni fakultet), Mina Čeperković (Univerzitet u Beogradu – Pravni fakultet)

Uređivački odbor:

Sava Vojnović (Univerzitet u Beogradu – Pravni fakultet), Aleksandar Cvetković (Univerzitet u Beogradu – Pravni fakultet), Mina Kuzminac (Univerzitet u Beogradu – Pravni fakultet), Marija Vlajković (Univerzitet u Beogradu – Pravni fakultet)

Naučni odbor:

prof. dr Bojan Spaić (Univerzitet u Beogradu – Pravni fakultet), prof. dr Miodrag Jovanović (Univerzitet u Beogradu – Pravni fakultet), prof. dr Đorđe Pavićević (Univerzitet u Beogradu – Fakultet političkih nauka), prof. dr Marija Karanikić Mirić (Univerzitet u Beogradu – Pravni fakultet), prof. dr Goran Dajović (Univerzitet u Beogradu – Pravni fakultet), prof. dr Tanasije Marinković (Univerzitet u Beogradu – Pravni fakultet), doc. dr Biljana Đorđević (Univerzitet u Beogradu – Fakultet političkih nauka), prof. dr Danilo Vuković (Univerzitet u Beogradu – Pravni fakultet), doc. dr Miloš Zdravković (Univerzitet u Beogradu – Pravni fakultet), doc. dr Milena Đorđević (Univerzitet u Beogradu – Pravni fakultet)

Međunarodni uređivački odbor:

Luka Burazin (University of Zagreb), Damir Banović (University of Sarajevo), Kenneth Einar Himma (University of Washington), David Duarte (University of Lisbon), Pierluigi Chiassoni (University of Genova), Andrej Kristan (University of Girona), Marko Milanović (University of Nottingham), Victor Garcia Yzaguirre (University of Đirona)

Prethodni članovi:

Milica Ristić (Univerzitet u Beogradu – Pravni fakultet), Andrej Confalonieri (University of Leiden), Teodora Miljojković (Centralnoevropski univerzitet), Stefan Rakić (Univerzitet u Strazburu), Nikolija Nedeljković (Univerzitet u Beogradu – Pravni fakultet).

Lektura i korektura radova na srpskom jeziku

Irena Popović

Priprema teksta

Dosije studio, Beograd

ISSN 2560-3663 (Online)

Publisher:

Center for Legal Fundamentals,
Serbian Association for Legal and Social Philosophy (IVR Serbia),
Faculty of Law University of Belgrade

Editor in chief:

Dr. Julieta Rabanos
(University of Belgrade – Faculty of Law)

Executive Editors:

Ana Zdravković
(University of Belgrade – Faculty of Law)
Mila Đorđević
(University of Belgrade – Faculty of Law)

Student Editorial Board:

Petar Mitrović (University of Belgrade – Faculty of Law), Fani Spalević (University of Belgrade – Faculty of Law), Mina Čeperković (University of Belgrade – Faculty of Law)

Editorial Board:

Sava Vojnović (University of Belgrade – Faculty of Law), Aleksandar Cvetković (University of Belgrade – Faculty of Law), Mina Kuzminac (University of Belgrade – Faculty of Law), Marija Vlajković (University of Belgrade – Faculty of Law)

Scientific Committee:

Prof. Dr. Bojan Spaić (University of Belgrade – Faculty of Law), Prof. Dr. Miodrag Jovanović (University of Belgrade – Faculty of Law), Prof. Dr. Đorđe Pavićević (University of Belgrade – Faculty of Political Science), Prof. Dr. Marija Karanikić Mirić (University of Belgrade – Faculty of Law), Prof. Dr. Goran Dajović (University of Belgrade – Faculty of Law), prof. Dr. Tanasije Marinković (University of Belgrade – Faculty of Law), Prof. Dr. Biljana Đorđević (University of Belgrade – Faculty of Political Science), Prof. Dr. Danilo Vuković (University of Belgrade – Faculty of Law), Prof. Dr. Miloš Zdravković (University of Belgrade – Faculty of Law), Prof. dr Milena Đorđević (University of Belgrade – Faculty of Law)

International Editorial Board:

Luka Burazin (University of Zagreb), Damir Banović (University of Sarajevo), Kenneth Einar Himma (University of Washington), David Duarte (University of Lisbon), Pierluigi Chiassoni (University of Genova), Andrej Kristan (University of Girona), Marko Milanović (University of Nottingham), Victor Garcia Yzaguirre (University of Girona)

Previous members:

Milica Ristić (University of Belgrade – Faculty of Law), Andrej Confalonieri (University of Leiden), Teodora Miljojković (Central European University), Stefan Rakić (Strasbourg University), Nikolija Nedeljković (University of Belgrade – Faculty of Law).

Proofreading (Serbian)

Irena Popović

Typesetting and Layout

Dosije studio, Beograd

ISSN 2560-3663 (Online)

SADRŽAJ

Trong Hiep Dinh, Phuong Chi Nguyen
Protecting National Sovereignty in Cyberspace within the Context of Digital Globalization – Regulations of Some Countries and Proposals 5

Marija Vranić
Legal Potential of Digital Assets in the Light of Companies' Business Operations 31

Sofija Lekić
The Impact of Digital Technologies on the Cultural Rights of D/Deaf and Hard-of-Hearing People 55

Dušan Samardžić
A Deleuzian Perspective on the Right of Data Protection on Social Media 85

Marija Vojisavljević
Evropska regulacija zaštite podataka na internetu 105

Nataša Ranković
Krađa identiteta kao krivično delo: *de lege lata* i *de lege ferenda* . . . 123

UDK 34/384.3
DOI 10.51204/IVRS_24101A

Trong Hiep Dinh*

Phuong Chi Nguyen**

PROTECTING NATIONAL SOVEREIGNTY IN CYBERSPACE WITHIN THE CONTEXT OF DIGITAL GLOBALIZATION – REGULATIONS OF SOME COUNTRIES AND PROPOSALS

The explosive growth of digital technologies is creating a virtual and borderless environment, which is so-called "cyberspace". In addition to serving as a platform that allows digital communication, information sharing, and online activities to take place, cyberspace carries various risks and vulnerabilities that can pose significant challenges to individuals, organizations, and even the nation. Throughout history, international law has built the concept of state sovereignty based on material aspects. However, digital globalization has significantly changed social relations, challenging important legal concepts that underlie international relations, including the concept of national sovereignty. Therefore, the issue of national sovereignty in cyberspace needs to be studied more carefully, thereby seeking appropriate solutions to protect national sovereignty in cyberspace.

Keywords: *Cyberspace Security, Digital Globalization, International law, National Law, National Sovereignty.*

1. INTRODUCTION

In June 2009, Robert Gates – the U.S. Secretary of Defense in an attempt to recommend the U.S. President to establish the U.S Cyber-Command (USCYBERCOM) as part of the U.S. Strategic Command (USSTRATCOM) has forecasted: "The next war will begin in cyberspace" (Army News Service 2009). This anticipation gradually becomes true as cyberspace security is currently one of the key agendas

* Research fellow at Hanoi Law University, tronghiepdinh153@gmail.com.

** Research fellow at Foreign Trade University, phuongchinguyen02@gmail.com.

in the Defense Policies of governments. In fact, there have been many cases where countries have become victims of cyber attacks. In 1982, a logic bomb was installed by the U.S. Central Intelligence Agency (CIA) into the computer system controlling the Soviet gas pipeline, causing a shocking explosion in Siberia (Heather Dinniss 2012, 6). In 2007, the homepages of the Estonian Government, banks, and television stations became a target of denial of service (DoS) attacks, resulting in removal of the original content (Marco Roscini 2012, 5). Notably, a computer worm called Stuxnet attacked Iran's industrial infrastructure in 2010 with the purpose of destroying centrifuges at the Natanz nuclear enrichment facility. Although the consequences of the incident have not yet been clearly announced, Iran had to temporarily suspend the uranium enrichment process at Natanz, according to the International Atomic Energy Organization (IAEA) (Broad 2010). The list of victims of cyber attacks will definitely continue to expand in the context of increasingly complicated international relations.

If the next war will indeed be in cyberspace, then what should the international community do about it? Having all this in mind, the authors decided on the topic "Protecting national sovereignty in cyberspace within the context of digital globalization – regulations of some countries and proposals" in order to analyze the above-mentioned issues more clearly and suggest some proposals for parties to secure the national security on cyberspace. The paper will clarify the following legal issues related to national sovereignty in cyberspace.

Firstly, the paper will analyze international law developments on cyberspace security. The international law on cyberspace security has undergone a long period of development and application since the 20th century when governments gradually realized the rapid advancement of information technology and widespread usage of the Internet. As a result, the issue of how cyberspace should be regulated has become a severe concern in countries worldwide. Accordingly, the paper will elucidate and analyze the process of developing international law on cyberspace security, including the process of analyzing, discussing among countries, and reaching an agreement on this issue. After analyzing the developments of international law on cyberspace security, the paper will clarify and analyze the importance of protecting sovereignty in cyberspace within the context of digital globalization.

Secondly, the paper will review the intricate landscape of regulations aimed at safeguarding national sovereignty in the realm of

cyberspace. By examining the legal frameworks implemented by various countries around the world, the paper aims to shed light on the diverse approaches taken to address this pressing issue. In particular, we shall explore different strategies employed by different countries to secure their digital borders, mitigate cyber threats, and preserve their national interests.

Thirdly, the paper will analyze some contrasting views of countries on ensuring cyberspace security, in terms of policies, countermeasures, etc. After analyzing the international laws as well as domestic laws of countries, regarding the protection of sovereignty in cyberspace, the paper will point out and evaluate contrasting views that still exist between countries on this issue. These inadequacies arise in the process of exchange and negotiation processes aimed at improving the effectiveness of protecting the country's sovereignty in cyberspace. These contrasting views are part of the reason why the protection of the country's sovereignty in cyberspace is not yet effective and still appears to have shortcomings.

Fourthly, the paper will propose a range of solutions aimed at safeguarding governmental sovereignty in cyberspace. These solutions may encompass the development of robust cybersecurity frameworks, the establishment of international cooperation and information-sharing mechanisms, the implementation of effective legislative measures, and the nurturing of a skilled cybersecurity workforce. Through these proposed solutions, governments can aspire to preserve their sovereignty, ensuring the security, stability, and integrity of their digital domains.

2. THE DEVELOPMENT OF INTERNATIONAL LAW ON CYBERSPACE SECURITY

2.1. The development of international law on cyberspace security

Since the late 1990s, the United Nations (UN) has attempted to identify and assess the challenges that the digital revolution brings. Accordingly, the UN General Assembly has issued various annual Resolutions related to information security, affirming that "the spread and use of information technology and equipment can affect the interests of

the entire international community" (Nguyen Tien Duc, Tran Thi Thu Thuy 2019), and "intentional misuse of these technologies could have dangerous implications for all nations" (Resolution No. 55/63/2000, UN General Assembly).[1] Deriving from this spirit, the UN General Assembly has endorsed the holding of the 1st World Summit on the Information Society. The Geneva Declaration of Principles and Geneva Plan of Action adopted at the Summit matched an important milestone when the international community made stipulations about the basic principles of internet-based information society and internet governance. Article 49 of the Declaration recognized the sovereign right of States for Internet-related public policy issues.[2]

Then, in 2004, the UN established the Group of Governmental Experts (GGE) on "Developments in the Field of Information and Telecommunications in the Context of International Security" in order to examine existing and potential threats arising from the use of Information and Communications Technologies by States, and considered actions to address them, including norms, rules, principles and confidence-building measures. In June 2013, the UN has published the third report of the Group, stating that "state sovereignty and international norms and principles that flow from sovereignty apply to state conduct of Information and Communications Technologies – related activities, and to their jurisdiction over Information and Communications Technologies infrastructure within their territory".[3] This statement of the GGE points out that application of state sovereignty is embodied in the following two levels: *First*, in a technical level, state sovereignty applies to Information and Communications Technologies infrastructure, which is located in the level of "cyber" including the internet, telecommunication networks and communication systems, communication systems and radio and television networks, computer systems, and embedded processors and controllers in key industrial facilities. *Second*, in a social level, state sovereignty applies to Information and Communications Technologies activities, which is located in the level of "space", that is, activity forms on the platform of Information and Communications Technologies system (Fang 2018, 80).

[1] UN General Assembly Resolution No. 55/63 of December 4, 2000.

[2] Geneva Declaration of Principles 2003, Paragraph a, Art. 49.

[3] UN General Assembly, 2013 UN GGE Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Article 20.

Besides the UN, international organizations also make efforts to research the impact of digital technology on international security and stability. One of the notable documents is the Budapest Convention on Cybercrime, signed in November 2001 and officially taking effect in 2004. Currently, this is the only binding international document relating to cybercrime acts. Accordingly, the Budapest Convention divides cybercrime into four groups: violations of the confidentiality, integrity and availability of computer data and computer systems; computer-related crimes; crime-related content; infringe copyright and neighboring rights. Also, each Party of the Convention shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held accountable for a criminal offense established in accordance with this Convention, committed for their benefit by any natural person (European Treaty Series – No. 185/ 2001; Council of Europe).[4]

Reputable jurists in the field of international law have also provided useful opinions and suggestions related to cyberspace security issues. In early 2017, Michael Schmitt published the document "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations" (2017). The guide outlines how international law applies to cyber activities in peacetime and war conflicts, and analyzes common cyber incidents that countries face every day.

It is evident that the international community currently lacks a widely disseminated international document regulating cyberspace, cyber security and its related legal issues. Most countries are implementing their own cyberspace governance activities within their territories, maintaining benefits and limiting challenges from cyberspace. Negotiating on an international document related to this issue is considered too soon for some countries due to disputes over the interests and obligations of the parties. As such, states currently claim to rely on the principles of the UN Charter and other relevant documents in resolving issues related to cyberspace security.

2.2. The importance of protecting national sovereignty in cyberspace within the context of digital globalization

The rapid development of the Internet has revolutionized the functioning of nations and societies, driving economic progress, facilitating communication, and fostering innovation. However, with these

[4] Convention on Cybercrime, section 1, Council of Europe, *European Treaty Series* No. 185/2001.

advancements come inherent challenges, particularly in maintaining national sovereignty in cyberspace. Since countries become increasingly interconnected, the significance of protecting national sovereignty in cyberspace cannot be overstated.

First, national sovereignty is the cornerstone of a nation's identity, enabling countries to have the right to govern their internal affairs without external interference, contributing to peace and stability in international relations. National sovereignty serves as the foundation for international cooperation and provides the legal framework for treaties and agreements. Therefore, respecting and protecting national sovereignty is always the utmost priority for countries to maintain the autonomy and rights of individual nations within the global community.

Second, the nature of cyberspace allows information to flow freely, regardless of geographical boundaries, creating an interconnected and expansive domain. This borderless nature exposes inherent risks, as cyber threats can emerge from any corner of the globe, rapidly crossing national borders and attacking national sovereignty. Cyberspace has become a new battleground for both state-sponsored and non-state actors. Without adequate protection, national sovereignty can be compromised, leaving governments vulnerable to cyberattacks, data breaches, and malicious interference. Several recorded instances during the past decade have demonstrated the vulnerability of nations to cyber attacks. Numerous countries, including Kyrgyzstan, South Korea, Switzerland, England, and the U.S, have also reported being victims of cyber attacks. With the complexity of international relations increasing, it is expected that the list of cyber attack victims will continue to expand. Hence, the protection of national sovereignty in the digital realm plays an important role in safeguarding a nation's critical infrastructure, such as power grids, transportation systems, and communication networks. The integrity of these systems is paramount, as any breaches can result in severe consequences, including the disruption of essential services and compromising national security. By upholding sovereignty, governments can implement robust cybersecurity measures and effectively counter cyber threats arising from both domestic and international origins.

Third, preserving national sovereignty in cyberspace enables countries to design and implement policies that effectively and prop-

erly adapt to their own needs and circumstances. It grants countries the ability to navigate the ever-changing digital landscape, create regulatory frameworks, and devise national strategies concerning cybersecurity, digital infrastructure growth, and technological advancement. By safeguarding sovereignty, countries can assert their control over the digital domain, guaranteeing that decisions made align with the welfare and interests of their own government and citizens.

Fourth, during the period of international economic integration, the economies heavily depend on interconnected networks and digital platforms. As a result, preserving national sovereignty in cyberspace plays a crucial role in ensuring a nation's economic stability. Governments must have the authority and capacity to regulate and safeguard their digital markets, intellectual property, and other sensitive economic data/assets. Without well-protecting sovereignty, countries face the risk of relinquishing control over their economic resources, making them vulnerable to economic espionage and unfair competition. By protecting sovereignty, governments can ensure fair and secure digital trade, promote domestic industries, and foster innovation to drive economic growth.

Fifth, cyberspace has become a global platform where ideas, values, and cultural expressions are freely exchanged. Therefore, protecting national sovereignty in cyberspace allows governments to preserve their cultural identity and protect their citizens' cultural values. Nations have the right to govern and control the content and information circulating within their borders to ensure that it aligns with their cultural and societal norms. This not only serves to preserve their cultural heritage but also contributes to maintaining security, political stability, and safeguarding national interests. By exercising sovereignty in cyberspace, governments can effectively manage the digital realm in a manner that respects their culture and preserves their socio-political fabric.

As stated in the introduction, Robert Gates' forecast of "The next war will begin in cyberspace" cannot be more accurate at the present time. This encourages countries to enhance their awareness of the importance of cyber sovereignty and, at the same time, requires them to invest appropriate resources in protecting cyber sovereignty as they have traditionally done in military competition.

3. DIFFERENT APPROACHES OF COUNTRIES ON THE PROTECTION OF CYBERSPACE SOVEREIGNTY

It is widely acknowledged that international law concepts, including the fundamental principles of sovereignty and non-intervention, are considered applicable to the actions of states in cyberspace (Harriet Moynihan 2019). However, the practical application of these principles and their interpretation by different countries remain the subject of ongoing debate. The absence of a consensus on how international law should be applied to states' cyber activities has resulted in legal ambiguity and triggered many jurisdictions to establish their own framework to protect national security and sovereignty.

In this regard, States will normally exercise their sovereign powers by controlling and regulating cyberinfrastructure in their territory exclusively and independently. Some states choose to regulate certain aspects of cyber activity in their territory, for example, through laws about the processing of personal data and permissible content on the internet, while others exert tighter controls over access to the internet and personal data. This paper will then discover different strategies employed by different legislations to secure their digital borders, mitigate cyber threats, and preserve their national interests.

3.1. The legal frameworks on cyberspace sovereignty implemented by some countries in the world

3.1.1. The United States

The United States (U.S.) have asserted that sovereignty is only a principle rooted in international law, and therefore, no regulations or guidelines need to be derived from this principle that would be applicable specifically to cyberspace (Harriet Moynihan 2019). Unlike the conventional framework of sovereignty, which encompasses territorial, aerial, and maritime domains where States assert their power through domestic laws, the internet or cyberspace, in its entirety, appears to transcend physical limitations. It only functions as a virtual network connecting nodes, lacking a tangible existence that can be constrained by geographic or physical boundaries, thus challenging the notion of territorial sovereignty or control by any particular state (Adams, Jackson, Mohamad Albakajai 2016).

The U.S. has a long history of taking a relatively hands-off approach to cyberspace regulation compared to some other countries. While there are laws and regulations related to cybersecurity and data protection, such as the Computer Fraud and Abuse Act, the Federal Information Security Management Act, or The Federal Trade Commission Act, these do not touch much on the sovereignty aspects, giving room to promote a free and open internet. Some explain the reason behind this is that the early designers and developers of internet technology had a political desire to satisfy the wishes of the capitalists in the U.S. (James Lewis 2010, 55–65). Which, the primary purpose was to limit the governmental powers by establishing a globally accessible network that operates without a central command node, promoting a stateless and open connection across the world (Gary Schneider 2013). The view that cyberspace is a Global Commons, thereby falling outside the jurisdiction of any specific country, is reiterated scatter in various official documents of the U.S. government, as well as in statements made by non-governmental organizations (NGOs) operating within the country. Specifically, in the 2018 National Defense Strategy (Association of the U.S. Army 2008), the U.S. Secretary of Defense only set out their Domain Preeminence over the land, air, and sea, while putting the data transmitted via sea or air in the discussion of global commons. In the 2018 National Cyber Strategy, President Donald J. Trump repeatedly used the term "global" when discussing the nature of cyberspace. Some scholars did support such view, by proving that (i) the IP address, a unique numerical identifier assigned to devices connected to a computer network; (ii) the DNS, a decentralized naming system that translates human-readable domain names; and (iii) the cyberspace and the connection therein are the common resources brought out by the Internet, but not by any specific government. In terms of the NGO's viewpoints, A Declaration of the Independence of Cyberspace by John Perry Barlow, the founder of Electronic Frontier Foundation (EFF), is a notable statement. The EFF is a non-profit organization based in the U.S. that champions civil liberties and digital rights in the realm of technology. In the Declaration, John asserts that the governments have no sovereignty over cyberspace, which he called "the new home of Mind," and "the global social space people are building to be naturally independent of the tyrannies the government seek to impose on" (John Barlow 1996).

However, the above does not mean that the U.S. has given up its right to claim sovereignty in cyberspace. On the contrary, as cyber attacks on government organizations are increasing, the country has been more focused on protecting critical infrastructure from cyber threats and addressing issues such as misinformation and cybercrime. Increasingly, senior the U.S. government officials have acknowledged this duty with respect to activities in cyberspace. In 2012, State Department Legal Adviser Harold Koh offered the first major statement on this matter, emphasizing that "States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict. The physical infrastructure that supports the Internet and cyber activities is generally located in a sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered" (Harold Koh 2012). From a military perspective, General Keith Alexander – former Director of the U.S. National Security Agency, and the first commander of the USCYBERCOM said that the cyber sovereignty concept must serve a strategic goal of ensuring the freedom of action of the U.S. and its allies in cyberspace and denying the same rights to adversaries (Cynthia Ayers 2016). In later years, USCYBERCOM also declared that the U.S. will treat cyber attacks in the same manner as conventional attacks, and will exercise the interceptive self-defense rights as stipulated under Article 51 of the UN Charter, and even the anticipatory and preemptive self-defense, to best protect the States' interest (Geoffrey S. DeWeese 2015).

3.1.2. The United Kingdom

Situated in a distant geographical location, the United Kingdom (U.K.) somehow shares the same approach to cyber sovereignty as the U.S. The U.K. has long been known to possess a significant level of expertise and influence in the application of international law to the realm of cyberspace. A noteworthy development, however, was first witnessed in 2018 during a discourse delivered by the former Attorney General, Jeremy Wright, at the esteemed Chatham House. Surprisingly, Wright expressed an unconventional standpoint by rejecting the existence of a governing principle of sovereignty applicable to cy-

ber operations. The U.K. maintains that while sovereignty is a fundamental principle in international law, it does not provide a sufficient or clear basis for establishing specific rules or additional prohibitions for cyber conduct, and asserts that relying solely on the broad concept of sovereignty is insufficient for developing a comprehensive framework that effectively governs cyber operations beyond the principle of non-intervention (Michael Schmitt 2022). By adopting this viewpoint, the U.K. maintains that the prohibition on intervening in the internal or external affairs of other states serves as the fundamental criterion for evaluating acts of internationally wrongful conduct in the majority of cyber operations conducted remotely. This position allows the U.K. to conduct cyber operations in another state's territory without violating sovereignty, as long as it does not exceed the boundaries of non-intervention.

After such controversial speech, the U.K. subsequently issued two additional statements pertaining to the role of international law in cyberspace. These include a declaration made in 2021 for the UN GGE on cyberspace and a speech delivered in May 2022 by the current U.K Attorney General, Suella Braverman, at Chatham House. While there have been limited changes in the U.K.'s stance since 2018, each statement has contributed to a more detailed delineation of the U.K.'s positions on this matter. Specifically, the 2021 UN GGE statement by the U.K., reiterated the U.K.'s position on sovereignty, while none of its NATO allies, including the U.S., followed suit. The statement acknowledged the existence of differing opinions on sovereignty but emphasized that such differences should not hinder states from evaluating whether specific situations constitute internationally wrongful acts and reaching common understandings on those matters. Regarding the application of the UN Charter, the statement recognized that the prohibition on the use of force and the right to self-defense in response to an armed attack also extend to the cyber domain. However, it did not explicitly address whether cyber operations that are non-destructive or non-injurious could be considered as a use of force or an armed attack. Instead, it suggested that if cyber operations produce effects similar to those caused by kinetic actions that qualify as a use of force or an armed attack, they would be treated likewise. Following by GGE reports, Attorney General Suella Braverman reiterated the U.K.'s stance on non-intervention and discussed the concept of coercion and collective measures in cyber operations in her speech before Chatham House in 2022. The Attorney General emphasized that states should not co-

ercively interfere in the affairs of others. Coercion was thereby defined as depriving a state of control over its "domaine réservé", which refers to areas where international law allows states to make decisions freely, and cyber operations disrupting this control were deemed unlawful. The speech acknowledged the evolving definition of coercion and the ongoing debate on collective countermeasures, without taking a firm stance. In general, the U.K. aligns with mainstream views on how international law applies to cyberspace, except for its stance on sovereignty. However, as more states adopt a different perspective and the U.K. is likely to seek common in defining unlawful cyber operations, the significance of this disagreement is diminishing rapidly (Michael Schmitt 2022).

3.1.3. Russia

Russian leaders perceive cyberspace as a critical arena in the global power struggle, attributing special significance to it in terms of Russia's power and influence internationally. Consequently, Russia adopts a proactive stance on cyberspace sovereignty, positioning itself as being "one step ahead" in this field. In the context of "Russia is facing cyber threats of a military, criminal, and terrorist nature, the most serious challenge to national security and international peace in the 21st century", as said by President Putin when signing a pact to create communication link on cyber security with the U.S. (Ellen Nakashima 2013), Russia is currently starting to build a concept of "cyberspace sovereignty" based on the sovereignty concept of the Russian Military Encyclopedia. Accordingly, these concept involves granting Russia powers to (i) exert control over the realms of "cyber engineering" and "cyberpsychology", which together constitute the two distinct aspects of cyber warfare; (ii) gain an advantage over adversaries and safeguard vital national assets by exercising control over devices in the realm of cybersecurity; (iii) exercise authority over the national cyberinfrastructure; and (iv) censor and manage the information in cyberspace (Digital and Cyberspace Policy Program and Net Politics 2020).

Russia has concretized its view on cyber sovereignty by implementing several domestic laws and regulations, including, but are not limited to: (i) Data Localization Law (2015), which requires personal data of Russian citizens collected by both domestic and foreign companies to be stored within the territory of Russia and grants Russian authorities access to such information; (ii) Federal Law on Counteract-

ing Terrorism (2016), which mandates telecommunications operators and internet service providers to retain user data for specified periods and provide access to security agencies upon request and requires encryption keys to be provided to authorities, which can have implications for user privacy and data security; (iii) Sovereign Internet Law (2019), which provides the Russian government with extensive control over the internet within its borders and grants Russian authorities the power to regulate and potentially isolate the Russian segment of the internet (Runet) in case of perceived external threats or emergencies, (iv) Information Security Law (2006, amended in 2019), which establishes a legal framework for information security and aims to protect critical information infrastructure within Russia and prevent cyber threats. For the most recent development, in 2019, Russian President Vladimir Putin approved a law requiring that all smartphones, computers, and smart TV sets sold in Russia must be equipped with pre-installed Russian software, which later came into force in July 2020. Also, in 2018, Russia also proactively put forward a resolution at the UN General Assembly, allowing legitimized state surveillance and censorship through its emphasis on sovereignty and non-interference in the internal affairs of countries. The resolution created an Open-ended Working Group (OEWG) on the topic of cybersecurity to run parallel to the already existing UN GGE, effectively bifurcating the discussion of cyber norms at the UN. This could allow Russia to use the OEWG as a forum to reinterpret previous UN GGE reports to better align with Russian preferences for internet governance. Within internet governance, Russia has enacted measures to impede access to select websites and control online content deemed to contravene Russian legislation or pose a risk to national security. The government possesses the capability to direct internet service providers to block access to particular web addresses or even entire platforms. Russia also maintains stringent regulations governing online content, granting the government the authority to prohibit websites and social media platforms that are perceived to disseminate illicit or detrimental information. The above efforts have clearly demonstrated Russia's views on cyberspace sovereignty.

3.1.4. China

Echoing with its neighbor Russia, on this matter, China is well-known for having strict regulations on cyberspace. Since 2013, cyber security has become one of the most important issues on the agenda of

the Grand National Security strategy, especially after the founding of a new Working Group on Cyber Security and ICT, which directly led President Xi Jinping to meet the challenges and threats rising within cyberspace (Shen Yi 2014, 41– 43). Since then, President Xi and the Chinese government have set a major goal for China in cyberspace, which is to transform China into a cyber power where increasing not only effectively defends against potential cyber threats but also China influences shaping the global rules governing cyberspace (Cyberspace Administration of China 2015). However, in his speech to China's Second World Internet Conference in 2015, President Xi called on countries to respect each other's cyberspace sovereignty and different governance models, and no country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security" (Xi Jinping 2015). In 2016, Chinese Ambassador Liu Xiaoqing, speaking at the "Cyber 2016" Conference held in the U.K, also proposed that the concept of "equal sovereignty" enshrined in the UN charter should also be applied to cyberspace. These statements somehow reflect the understanding of the Chinese government of the concept of cyber sovereignty, which includes key components: (i) it emphasizes the state's authority to control the flow of information within its territory; (ii) it recognizes that each state has the autonomy to formulate its own policies regarding cyberspace; (iii) it highlights the principle that all states should have equitable participation in shaping the rules, norms, and code of conduct governing the global cyberspace and (iv) it underscores the significance of respecting sovereignty as a fundamental guiding principle in addressing international cyber-related matters (Xinhua Net 2014).

In light of the above, China has implemented several laws and regulations related to cyber sovereignty, some highlighted regulations can be named as (i) Cybersecurity Law implemented in 2017, which establishes the legal framework for safeguarding China's cyberspace sovereignty and requires network operators to ensure the security of their networks, protect user information, and cooperate with government authorities in matters related to cybersecurity; (ii) National Intelligence Law, enacted in 2017, which empowers Chinese intelligence agencies to gather intelligence on threats to national security, which includes information and communication systems; and specifically, (iii) National Security Law of China enacted in 2015, which clearly sets

out the protection of sovereignty in cyberspace is one of the tasks of ensuring national security. These legal instruments refers to the state's control and governance over the internet within its borders. Therefore, they aim to regulate online activities, safeguard national security, protect the rights of citizens, and promote Chinese values and interests in the digital realm. Besides, in support to such regulations, the country also operates a sophisticated system of internet censorship and content filtering known as the Great Firewall of China, employing various technical measures to block access to foreign websites and content deemed undesirable or politically sensitive. According to Ankit Kumar (2023), the Great Firewall is aimed at maintaining control over information flow and preventing the dissemination of content that could challenge the Chinese Communist Party's authority. Similar to Russia, China also imposes data localization mandates, which dictate that personal and significant data obtained within China's borders must be stored and managed on domestic servers, adhering to Chinese regulations and supervision. It should be noted there are several debates and criticism from international observers who argue that China is restricting freedom of expression, and privacy rights, and hinders open access to information, yet the Chinese government maintains its stance that these measures are necessary for national security and social stability.

3.1.5. South East Asia

Cybersecurity is a key enabler of the economic progress and betterment of living standards in the digital economy for Association of Southeast Asian Nations (ASEAN) countries. This has become even more apparent during and after the Covid-19 pandemic, which witnessed a rapid shift towards digitalization and the widespread migration of government, business, and social activities to online platforms. Given this trend, ASEAN countries altogether published a draft of the ASEAN Cybersecurity Cooperation Strategy for the years 2021–2025, which emphasizes the importance of cybersecurity in supporting the economic progress and well-being of ASEAN member states in the digital economy. The proposed strategy aims to ensure the security and stability of cyberspace through five dimensions of work, including (i) advancing cyber readiness cooperation, (ii) strengthening regional cyber policy coordination, (iii) enhancing trust in cyberspace, (iv) regional capacity building and (v) international cooperation. The draft also mentions the establishment of an ASEAN Cybersecurity

Coordinating Committee and the development of an ASEAN Computer Emergency Response Team (CERT) to enhance incident response capabilities. While waiting for the official publication of this strategy and other mutual agreements, individual ASEAN member states have their own national laws and regulations pertaining to cyberspace and cybersecurity. These laws may address various aspects such as data protection, online privacy, cybersecurity standards, cybercrime prevention, and digital governance.

In Vietnam, since 2021, the State has announced that sovereignty over cyberspace is an important part of national sovereignty, and ensuring sovereignty in cyberspace helps to protect national sovereignty (Vietnam News 2021). Speaking at the national scientific conference on "Ensuring national sovereignty in cyberspace", Associate Professor, Dr. Nguyễn Văn Thành, special Vice Chairman of the Central Theoretical Council, former Deputy Minister of Public Security, said that national sovereignty in cyberspace is a supreme, absolute and complete right (Vietnam News 2021). It is the responsibility of the State to exercise direct or indirect management and control over cyberspace through the implementation of policies, laws, and technological capabilities, which must be carried out in accordance with international laws and regulations. Within its own jurisdiction, Vietnam has set out its own legal framework on cyber security and cyber sovereignty, including (i) the Law on Cybersecurity, passed in 2018,[5] and (ii) Decree on Data Privacy, passed in 2023,[6] which grants authorities broad powers to monitor, control, and regulate online activities. These laws require service providers to store user data within Vietnam's territory and cooperate with government agencies in matters related to cybersecurity and information control. The Vietnamese government has also established specialized agencies and units, such as the Ministry of Public Security's Department of Cybersecurity and High-Tech Crime Prevention (A05), to enforce cybersecurity measures, combat cyber threats, and monitor online content.

Malaysia, like many other countries, acknowledges the significance of cyber sovereignty and has articulated its perspective on the subject. The Malaysian government underscores the necessity of retaining authority and overseeing cyberspace within its territorial boundaries to safeguard national security, uphold the integrity of its political system, and maintain social cohesion. Malaysia's approach to

[5] Law on Cyber security (Vietnam) No. 24/2018/QH14.

[6] Decree on Data Privacy (Vietnam) No. 13/2023/ND-CP.

cyber sovereignty involves enacting laws, regulations, and policies to govern and safeguard its cyberspace. The country has implemented (i) the Personal Data Protection Act to regulate the collection, use, and disclosure of personal data by organizations,[7] along with (ii) the Communications and Multimedia Act empowers the government to regulate and oversee the telecommunications and multimedia sectors, including online content and electronic transactions.[8] The Malaysian government also focuses on cybersecurity and has established agencies such as the National Cyber Security Agency (NACSA) to coordinate and enhance the country's cybersecurity efforts, aiming to protect critical information infrastructure and combat cyber threats. However, it is worth noting that Malaysia adopts an inclusive and balanced approach to governing cyberspace. On the one hand, the Malaysian government recognizes the significance of digital innovation, economic advancement, and the freedom of expression in the online realm, especially via developing an internal infrastructure known as the Multimedia Super Corridor (Toby E. Huff 2001, 439–458), which encompasses both a physical location and an electronic "cyberspace" aimed at promoting the growth of the information and communication technology industry in Malaysia. On the other hand, it also emphasizes that individuals and organizations have a responsibility to adhere to the laws and regulations in place to uphold cybersecurity and safeguard the overall welfare of the country.

Thailand has expressed its views on cyber sovereignty, emphasizing the need for government control and regulation over cyberspace to ensure national security, protect its political system, and maintain social order. Thailand has enacted various laws and regulations to exercise control over cyberspace and maintain cyber sovereignty, including (i) the Computer Crime Act and (ii) the Cybersecurity Act, which empower the government to regulate and monitor online activities, combat cyber threats, and protect critical information infrastructure. Similar to Vietnam and Malaysia, the Thai government has also established agencies such as the National Cybersecurity Committee, the NACSA, and the Electronic Transactions Development Agency to oversee and coordinate cybersecurity efforts. Online platforms and websites have been subject to government censorship and monitoring, and individuals have faced legal consequences for online activities deemed threats to national security or social order.

[7] Act 709 on Personal Data Protection 2010 (Malaysia).

[8] Act 589 on Communications and Multimedia 1998 (Malaysia).

3.2. The contrasting views of countries on ensuring the security in cyberspace

The development of international law pertaining to the seas has been a lengthy process spanning several decades, primarily due to varying perspectives and conflicting interests among maritime nations. Similarly, in the present day, countries continue to hold divergent views on the establishment of an international legal framework for ensuring national sovereignty and security in cyberspace.

According to the Permanent Delegation of the Socialist Republic of Vietnam in New York – the U.S. (2020), during the "Arria formula" meetings at the UN, countries have acknowledged the relevance of international law in addressing the use of information and communication technology. However, each country holds distinct positions on this matter. Australia and Japan, for instance, oppose the establishment of new rules and prioritize further discussions on the application of existing international law to cyberspace. Besides, the Ministry of Information and Communications of Vietnam (2023) points out that many Western countries currently do not support the development of new rules of international law in cyberspace. Among the existing rules, Western countries pay special attention to promoting the application of rules on responsible state behavior in cyberspace. Denmark and Nordic countries have emphasized that cyberattacks targeting critical infrastructure of other nations violate international law and norms of responsible state behavior. They strongly condemn such actions as "unacceptable". Also in this report, the U.S, the European Union, and Australia have highlighted the importance of state obligations to prevent malicious cyber activities from taking place within their borders in their respective statements. This aligns with the principles outlined in norms regarding responsible state behavior in cyberspace. Western countries also express their support for the "Action Program to promote responsible state behavior in cyberspace" put forward by France and Egypt, emphasizing the need for cooperation mechanisms (the Ministry of Information and Communications of Vietnam 2023).

In contrast, countries like China and Russia hold the view that new rules are necessary, reported from Allison Pytlak (2023). China, in particular, emphasizes the importance of broad participation in the formulation of new rules, with a specific focus on safeguarding the interests of developing nations. Among the existing rules of international

law, China highlights the significance of complying with the UN Charter and other principles of international law. They stress the need to prevent the "battlefieldification" of cyberspace in order to protect critical infrastructure. China advocates for adherence to principles such as sovereign equality, refraining from the use or threat of force, peaceful dispute resolution, and maintaining the peaceful nature of cyberspace.

Meanwhile, Russia argues that the application of existing rules to cyberspace predominantly serves the interests of powerful nations, thereby perpetuating the injustices present in the physical world. As a result, they advocate for the adoption of a new universal and legally binding convention that would address the perceived Western-centric nature of the current Internet. Russia specifically mentions a document it co-submitted to the UN on an updated version of the International Information Security Treaty.

In addition to the contrasting positions of the major factions, other countries expressed their concerns with varying perspectives in their statements. According to Allison Pytlak (2023), Qatar and Pakistan, for example, mentioned the need for the development of new rules in cyberspace. However, they emphasized that these new rules should be legally binding and take into account the consequences of violating them. Developing countries, especially those with limited cyber capabilities, view binding international rules as a more dependable safeguard. They believe that such rules provide a stronger guarantee for their interests and security in the cyber domain. Mozambique, rather than proposing new rules, highlighted the need to reassess the concept of cyber sovereignty, emphasizing that the existing capacity asymmetries in the physical world should not be replicated in cyberspace. This viewpoint aligns with Russia's perspective. Furthermore, Albania, Latvia, Brazil, and Pakistan utilized the occasion to appeal to the international community for support in enhancing network capacity in developing countries (the Security Council 2023). These countries recognize the significance of bridging the digital divide and ensuring that developing nations have the necessary resources to improve their cyber capabilities and participate more effectively in the digital realm.

Indeed, the aforementioned perspectives of various countries demonstrate the existence of divergent "factions" in the realm of international law in cyberspace. These differences in perspectives and conflicts of interest have contributed to the conflicting views during the process of establishing an international legal framework for ensuring security in cyberspace. The complex nature of cyberspace, coupled

with the diverse interests and concerns of different countries, present significant challenges in reaching a consensus on such a document. However, recognizing the importance of global cooperation and addressing the unique challenges of cyberspace is crucial for promoting stability, security, and the protection of rights and interests in the digital domain. Also, efforts to bridge the gaps and foster dialogue among nations are very important for advancing the development of an effective and inclusive international legal framework for cyberspace.

4. SOLUTIONS FOR COUNTRIES FOR SAFEGUARDING GOVERNMENTAL SOVEREIGNTY IN CYBERSPACE

4.1. Constructing international cooperation on cybersecurity

Without a doubt, enhancing the function of international organisations, enhancing the global network management system, and jointly ensuring network security are essential to promoting cooperation in cyberspace. Countries ought to work together more in fields of technical cooperation, combating cyberterrorism and cybercrime, and strengthening the Internet's multilateral, democratic, and open governance. This would progressively create a system in which cyberspace would become both beneficial to all nations and a fundamental component of cooperation.

Mutual respect, trust, equality, and benefit-sharing are essential for strengthening international cooperation and collaboration to confront emerging risks and difficulties. Organisations like the UN, the Shanghai Cooperation Organisation, the International Telecommunication Union, the BRIC countries, and the ASEAN Regional Forum are good places for nations to collaborate. These platforms have the potential to enhance national cooperation, foster peaceful dispute resolution, foster the establishment of international information security legal norms, and enable cooperation.

Coordination among relevant international organizations is also essential to ensure effective collaboration and address the complex and evolving landscape of cybersecurity. By strengthening these efforts, countries can promote greater cooperation, enhance security, and foster the sustainable development of cyberspace.

4.2. Enhance national capacity in ensuring security in cyberspace

Proactive steps are needed to prevent information technology misuse that could jeopardise international security and stability in order to create a "peaceful" cyberspace. It is imperative that we all refuse participating in an arms race in cyberspace and work to stop conflicts there. Rather, the emphasis ought to be on utilising cyberspace in a way that is consistent with humanity's shared interests. The UN Charter's tenets, which forbid using or threatening to use force, should be upheld by all states. This dedication contributes to effectively reducing the misuse of technology and averting disputes in cyberspace. Countries may help create a safe and secure cyberspace that benefits all people by adhering to these principles.

Thus, safeguarding cyberspace sovereignty entails putting in place strong policies that complement a nation's stature in the world and its network capacities. It comprises building robust defence and security mechanisms for networks, quickly identifying and thwarting network intrusions, and guaranteeing a strong basis for national network security. Building a network border through cooperation between military and civilian groups is both an immediate challenge for countries' digital sovereignty and a long-term cornerstone for maintaining it, much as geographical sovereignty requires strengthened defences. Building a strong cyberspace sovereign security capability requires the combination of military and civilian resources. This strategy acknowledges that the only way to successfully handle the difficulties associated with cyberspace security is through military and civilian collaboration. Measures such as military-civilian integration, dual-use technologies, and joint efforts are necessary to establish a coordinated cyberspace sovereign security force.

4.3. Develop the level of cybersecurity education for all walks of life

Improving cybersecurity education is essential to enhancing cyberspace security as a whole. Strengthening a few important areas can help accomplish this. First and foremost, it is critical to raise public awareness of cybersecurity issues by teaching people about typical dangers and offering advice on safeguarding personal data. Additionally, incorporating cybersecurity education into curricula and programmes

in schools can help cultivate a cybersecurity culture from a young age. Resources and training should be provided to educators so they can impart cybersecurity principles to students. Thirdly, in order to create a workforce with the necessary skills to tackle changing threats, it is imperative that cybersecurity education be improved for both professionals and current employees. This covers possibilities for ongoing professional growth, certifications, and specialised training programmes. Fourthly, targeted cybersecurity education and support programs for small and medium-sized enterprises (SMEs) can help them understand and mitigate risks. Additionally, cybersecurity education should target government officials and policy makers to enhance their understanding of cybersecurity issues. Lastly, promoting international cooperation and collaboration in cybersecurity education can facilitate knowledge sharing and capacity building among countries. By improving cybersecurity education in these areas, individuals, organizations, and nations can develop a strong cybersecurity awareness and expertise, contributing to a safer and more secure cyberspace for everyone.

5. CONCLUSION

In conclusion, as the world becomes increasingly interconnected and dependent on cyberspace, the protection of national sovereignty in this domain is of utmost importance. The potential for cyber warfare and the threats posed by malicious actors necessitate the development of effective governance and regulations. To secure national security in cyberspace, it is essential for countries to establish comprehensive legal frameworks that define the rights, responsibilities, and boundaries of states in cyberspace. These frameworks should address issues such as attribution of cyberattacks, the use of offensive cyber capabilities, and the protection of critical infrastructure. Furthermore, international cooperation and collaboration are vital in addressing the challenges of cyberspace. Countries should work together to develop common norms, standards, and principles that promote responsible state behavior in cyberspace. This includes fostering transparency, accountability, and trust among nations. At the same time, it is necessary to strike a balance between protecting national sovereignty and promoting digital globalization. Countries should avoid excessive restrictions that hinder the free flow of information and innovation, while ensuring that cyber-

security measures are in place to safeguard national interests. Most importantly, by working together and implementing effective measures, countries can safeguard their national security while promoting the benefits of digital globalization.

REFERENCE LIST

1. Adams, Jackson, Mohamad Albakajai. 2016. Cyberspace, A New Threat to the Sovereignty of the State. *https://core.ac.uk/reader/146502700* (last visited October 20, 2023).
2. Army News Service. 2009. Next war will begin in cyberspace, experts predict. *https://www.army.mil/article/17561/next_war_will_begin_in_cyberspace_experts_predict* (last visited 31 August, 2023).
3. Association of Southeast Asian Nations (ASEAN). 2021. Asean Cybersecurity Cooperation Strategy (2021–2025). *https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021–2025_final-23–0122.pdf* (last visited November 5, 2023).
4. Association of the U.S Army. 2008. The 2008 National Defense Strategy: Implications for the U.S Army. *https://www.ausa.org/sites/default/files/TBIP-2008-The-2008-National-Defense-Strategy-Implications-for-the-United-States-Army.pdf* (last visited October 20, 2023).
5. Ayers, Cynthia E. 2016. Rethinking Sovereignty in the Context of Cyberspace. *https://media.defense.gov/2023/Oct/02/2003312498/-1/ 1/0/RETHINKING%20SOVEREIGNTY.PDF* (last visited October 25, 2023).
6. Allison, Pytlak, Shreya, Lad. 2024. The UN Security Council Discusses Cyber Threats to International Security. *https://www.stimson.org/2024/un-security-council-cyber-threats-to-international-security/* (last visited April 15, 2024).
7. Barlow, John Perry. 1996. A Declaration of the Independence of Cyberspace. *https://www.eff.org/cyberspace-independence* (last visited October 25, 2023).
8. Binxing, Fang. 2018. *Cyberspace Sovereignty Reflections on Building a Community of Common Future in Cyberspace*. Beijing: Science Press Beijing.
9. Broad, William. 2010. Report Suggests Problems With Iran's Nuclear Effort. NY Times, *https://www.nytimes.com/2010/11/24/world/middleeast/24nuke.html, NYTimes* (last visited 31 August, 2023).
10. *Cyberspace Administration of China*. 2015. The Cyber Perception of President Xi Jinping: To build a cyber power, and let the development benefit the people. *http://www.cac.gov.cn/2015–12/10/c_1117414086.htm* (last visited November 5, 2023).

11. DeWeese, Geoffrey S. "Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenge of Imminence" (2015) 7th International Conference on Cyber Conflict. *https://ccdcoe.org/uploads/2018/10/Art-06-Anticipatory-and-Preemptive-Self-Defense-in-Cyberspace-The-Challenge-of-Imminence.pdf* (last visited October 25, 2023).
12. Digital and Cyberspace Policy Program and Net Politics. The Sinicization of Russia's Cyber Sovereignty Model. *https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model* (last visited October 30, 2023).
13. European Commission. 2022. European Cybersecurity Investment Platform. *https://www.eib.org/attachments/lucalli/20220206-european-cybersecurity-investment-platform-en.pdf* (last visited October 4, 2023).
14. Harrison Dinniss, Heather. 2012. *Cyber Warfare and the Laws of Wars*, New York: Cambridge University Press.
15. Huff, Toby E. 2001. Globalization and the Internet: Comparing the Middle Eastern and Malaysian Experiences. *Middle East Journal* 55: 439–458.
16. Koh, Harold. 2012. Remarks at the U.S. Cyber Command Inter-Agency Legal Conference. *http://opiniojuris.org/2012/09/19/harold-koh-on-international-law-in-cyberspace/, https://perma.cc/MJS5-XJVA* (last visited October 25, 2023).
17. Kumar, Ankit. 2023. Internet Censorship in China: The Struggle to Swat "Flies" Away. *https://icsin.org/blogs/2023/10/10/internet-censorship-in-china-the-struggle-to-swat-flies-away-2/* (last visited November 5, 2023).
18. Lewis, James Andrew. 2010. Sovereignty and the role of government in cyberspace. *The Brown Journal of World Affairs* 16: 55–65.
19. Ministry of Information and Communications. 2023. The UN discusses cyber attacks on critical infrastructure. *https://mic.gov.vn/pages/tintuc/printpage.aspx?tintucID=158845* (last visited November 5, 2023).
20. Moynihan, Harriet. 2019. The Application of International Law to State Cyberattacks Sovereignty and Non-intervention. Chatham House report. *https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/1-introduction* (last visited October 20, 2023).
21. Nakashima, Ellen. 2013. U.S. and Russia sign pact to create communication link on cyber security. The Washington Post. *https://www.washingtonpost.com/world/national-security/us-and-russia-sign-pact-to-create-communication-link-on-cyber-security/2013/06/17/ca57ea04-d788–11e2–9df4–895344c13c30_story.html* (last visited October 30, 2023).
22. Nguyen, Tien Duc, Thi Thu Thuy Tran. 2019. Cyber attacks and the principle of prohibition of the use of force in international law. *https://iuscogens-vie.org/2019/04/20/131/#_ftn14* (last visited October 4, 2023).
23. Permanent Delegation of the Socialist Republic of Vietnam in New York – United States. 2019. The UN Security Council discussed the issue of cyberspace stability. *https://vnmission-newyork.mofa.gov.vn/vi-vn/News/*

ConsulateNews/Trang/Hội-đồng-Bảo-an-LHQ-thảo-luận-vấn-đề-ổn-định-không-gian-mạng.aspx?p=38 (last visited November 5, 2023).

24. President of the U.S. 2018. National Cyber Strategy of the U.S of America. *https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf* (last visited October 25, 2023).
25. Roscini, Marco. 2012. *Cyber Operations and the Use of Force in International Law*, Oxford: Oxford University Press.
26. Schmitt, Michael. 2022. The United Kingdom on International Law in Cyberspace *https://www.ejiltalk.org/the-united-kingdom-on-international-law-in-cyberspace/* (last visited October 30, 2023).
27. Schmitt, Michael. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
28. Schneider, Gary P. 2013. *E-Business*. India: Cengage India.
29. Schultz, David, Nataliya Moroz. 2022. Cyberspace and the Future of International Law and Politics. International Policy Digest. *https://intpolicydigest.org/cyberspace-and-the-future-of-international-law-and-politics/* (last visited October 20, 2023).
30. Shen, Yi. 2014. Transform and construction: the design of national cybersecurity strategy and the capacity build in a post-Snowden age. *China Information Security* 5: 41–43.
31. United Nations. General Assembly. 2013. UN GGE Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *https://dig.watch/wp-content/uploads/A_68_98_E.pdf* (last visited October 15, 2023).
32. Vietnam News. 2021. Sovereignty over cyberspace an important part of national sovereignty: official. *https://vietnamnews.vn/society/1095123/sovereignty-over-cyberspace-an-important-part-of-national-sovereignty-official.html*, (last visited November 5, 2023).
33. Xinhua Net. 2014 Address of President Xi Jinping in the Brazil Congress. *http://news.xinhuanet.com/world/2014–07/17/c_1111665403.htm*. (last visited November 5, 2023).

UDK 004:316.323.6
DOI 10.51204/IVRS_24102A

Marija Vranić*

LEGAL POTENTIAL OF DIGITAL ASSETS IN THE LIGHT OF COMPANIES' BUSINESS OPERATIONS

In the introductory part of the paper, the most important explanations about the con-cept and nature of digital assets are given, serving as a guide in understanding the titled topic. The subsequent sections focus on some of the challenging practical issues related to it: whether digital assets can be a contribution to a company, can dividend be paid to shareholders in the form of digital assets, and what are the key conditions that companies must meet in order to provide digital asset services. The last lines of the paper summarize the findings and contain the observations on the legal and practical potential of digital assets in the context of compa-nies' business operations, both in current and the times to come. The research is conducted from the perspective of basic group of regulations of the Republic of Serbia, i.e. provisions that are most relevant for the analysis of the aforementioned questions.

Key words: *Companies Act, companies' business operations, digital assets, digital asset services, Law on Digital Assets*

1. INTRODUCTION

Companies' business operations are inseparable from the assets that companies own. The company's assets, as referred to in the Companies Act, comprise tangible and intangible assets owned by the company, as well as other company's rights.[1] More precisely, the company's assets consist of rights that the company has acquired by entering the contributions of its members,[2] through its business operations or

* The author is a bachelor of laws and a master's student at the University of Belgrade – Faculty of Law, *vranic.m.marija@gmail.com*.

[1] Companies Act – CA, *Official Gazette of the RS,* 36/2011, 99/2011, 83/2014 – other law, 5/2015, 44/2018, 95/2018, 91/2019 and 109/2021, Art. 44, Para. 1.

[2] Regardless of the legal form of the company, obligation to pay, i.e. to enter the contribution, is the foun-dation on which the company is built. Although the term

in another way (Jovanović, Radović, Radović 2021, 127), including the ownership right, company's claims and shares held in another company (Vasiljević 2019, 91). Determining what these assets comprise, as well as their value, is particularly important from the company law's perspective, since the CA regulates a set of le-gal situations to which the company's assets are related, both directly and indirectly.

Technological development "casts a shadow" over traditional understanding of the company's assets, giving rise to a (not so) new concept: the concept of digital assets. The digital era is rapidly moving on an upward trajectory, which indicated a clear need for the legal system to respond, through appropriate regulations, to the practical challenges it brings. One of the most important is the Law on Digital Assets, a relatively new law entirely devoted to its titled area.[3] This law is permeated with provisions that connect companies and digital assets in mul-tiple ways. In order to create a basis for considering this connection, the paper continues in the manner from the beginning: with a few key explanations, this time about *digital* assets, fol-lowed by an analysis (divided into separate sections) of whether digital assets can

"contribution" is used simplistically to denote a material good, legally speaking, a contribution is a subjective right that a member contractually transfers to the company in order to create its assets and enable the conduct of its activity (Jovanović, Radović, Radović 2021, 112, n. 130). In other words, the company, thanks to the fullfilment of this obligation (of course, and other prescribed condi-tions), "comes to life", while its business operations are gaining their full momentum. In addition, the payment, i.e. entry of contributions does not refer only to the creation of the company's assets, but also to the share capital increase by new contributions of existing company members or a member joining the company (CA, Art. 146, Para. 1, It. 1)). Furthermore and especially important, contributions enable the application of the *pro rata* principle to a number of rights and obligations of the company's members. Accordingly, a company member acquires a share in the company proportionately to the value of his contribution into the company's share capital (CA, Art. 151, Para. 1); unless provided otherwise in the memorandum of association, every member of the company has a voting right it the general meeting in the proportion to his share (CA, Art. 199, Para. 2); a stockholder is entitled to a pre-emption right to subscribe the stocks from a new emission on the day of adoption of the resolution on is-sue of stocks, in proportion to the number of the fully paid stocks of that class he holds on the day of adoption of the resolution on the issue of stocks, in relation to the total number of stocks of that class (CA, Art. 277, Para. 1); these are only some of the provisions in which the *pro rata* principle is incorporated. Previously outlined should serve as an aid in better understading of the paper's subtopic dedicated to considering whether a contribution to a company can be in the form of digital assets.

[3] Law on Digital Assets – LDA, *Official Gazette of the RS,* 153/2020. The law was passed at the end of 2020; its application in the Republic of Serbia has begun in the middle of the following year.

be a contribu-tion to a company, can dividend be paid to shareholders in the form of digital assets, and what are the key conditions that companies must meet in order to provide digital asset services. The last lines of the paper summarize the findings and contain the observations on the legal and practical potential of digital assets in the context of companies' business operations.

1.1. What are digital assets?

By passing the LDA, the Republic of Serbia joined the short list of countries that ex-panded their legislation to the new challenges of digital life, governing, in the first place, the issuance of digital assets, secondary trading in digital assets and the provision of services in connection with digital assets. The need to regulate these and other issues related to digital as-sets at the law level is becoming more pronounced and at some point will be inevitable (if it al-ready is not), but the practical reach of the subject law is questioned, giving the impression that its passing may have been rushed. Mihajlović points out that the regulation of digital assets can be considered unnecessary and premature at this moment, taking the position that the capital market, with which the digital asset market has the greatest similarities, is underdeveloped in Serbia (Mihajlović 2021a, 597). Motika is of the opinion that the LDA's provisions regarding the conduct and activity of digital asset service providers are to an extent similar to the ones that govern the permits' issuance for subjects operating on the financial market (Motika 2022, 109–110). Vujović suggests to refine the definition of digital assets, and believes that it is nec-essary to systematically work on the development of not only the digital asset market, but also the awareness of business entities regarding the possibilities available to them in terms of dig-ital assets (Vujović 2023, 80, 94).

Nevertheless, evaluating the law in that direction is not the subject of this paper, as it would require research that is significantly more complex and extensive than the one that re-sulted in the titled analysis. In any event, the fact is that, thanks to the development of digital technologies and relocation of a large number of activities from the "live" to the virtual space, which inevitably follows technological progress, the forms, ways of use and practical impor-tance of digital assets are passing through, it seems, a golden age. People nowadays are using digital assets for investment purposes, different services related to digi-

tal assets are provided and highly complex activities of issuance and secondary trading in digital assets are performed. At the same time, as it usually happens when life speeds up and overtakes existing legal frame-works, the task arises for law to adequately respond to changed or newly created circumstances, especially in the interest of legal certainty and suppression of possible abuses, which can leave particularly negative consequences in a legally unregulated field. Companies, the dominant participants on the market in both domestic and cross border operations, strive to keep their op-erations in step with modern trends, which, when it comes to digital assets, entails a series of legally very important questions that need to be answered. Therefore, it is justified to conclude that regulating, in the broadest sense, the use of digital assets, is not unnecessary, but that it is certainly a challenging and demanding task, which must be approached in detail, systematical-ly, and also innovatively, in an effort to find a balance between many advantages that are inher-ent in business operations related to digital assets and the risks of that operations that partici-pants in the digital asset market unavoidably face.[4]

According to the LDA, digital or virtual assets refer to a digital representation of value that can be digitally bought, sold, exchanged or transferred and used as a means of exchange or for investment purposes, whereby digital assets shall not include digital representation of fi-at currencies and other financial assets governed by other laws, unless otherwise provided by the LDA itself (LDA, Art. 2, Para. 1, It. 1). Digital assets can represent a substitute for some services in the field of bank-ing and capital markets, especially payment services and capital market investments (Jovanić 2021a, 21). This is not suprising considering that the provisions of the LDA that govern the is-suance of digital assets and secondary trading in digital assets, in their essence and objectives, are similar to the corresponding provisions of the Law on Capital Market,[5] and the relation be-tween the two laws could be

[4] What stands out the most when it comes to positive aspects od digital assets is the efficiency of financial transactions that are related to digital assets, given that they are conducted on a peer-to-peer basis, which, essen-tially, rules out the third parties (notably banks) that are operating under a traditional payment system, resulting in time savings and a reduction in overall transactions costs. The risks associated with digital assets can be classi-fied into several categories: market immaturity, market abuse, financial stability, financial crime and security risks (see Huang, Yang, Yang Loo 2020, 322–326).

[5] Law on Capital Market – LCM, *Official Gazette of the RS,* 129/2021.

considered in particular in terms of legal responsibility of the issu-er in the issuance of securities and digital assets (see Sovilj 2023).

There are two types of digital assets that the LDA regulates.[6]

1.1.1. Virtual currencies

Virtual currency is a type of digital assets that is not issued or guaranteed by a central bank or public authority, that is not necessarily attached to a legal tender and that does not have the legal status of money or a currency, but that is accepted by natural or legal persons as a means of exchange and can be bought, sold, exchanged, transferred and stored electronically (LDA, Art. 2, Para. 1, It. 2)). Virtual currencies can be understood also as "digital representations of value, issued by private developers and denominated in their own unit of account" (International Monetary Fund – IMF 2016, 7). In other words, virtual currencies have a different unit of account than national curren-cies. They are managed by private issuers and they may or may not have a monetary or account-ing value (Jovanić 2021b, 400). Considering the definition of virtual currencies from the begin-ning, it is safe to say that the LDA made a clear demarcation between virtual currencies and money, indicating that there should not be an equals sign between them. In practical terms, nevertheless, virtual currencies are used like money, which means, Motika concludes, that this activity *de facto* is a payment, while *de iure* it is not (Motika 2021).

Virtual currencies are – in the true sense of the word – decentralized. They do not have physical form and all activities involving them take place electronically,[7] under the conditions of a decentralized

[6] Mihajlović, in contrast, explains that there are three basic types of digital assets (see Mihajlović 2021a, 600–603).

[7] Digital assets are largely based on the so-called blockchain technology. The technology owns its sym-bolic name to the mechanism through which digital asset transactions are carried out, and which implies that the transaction data is entered into blocks that are "chained" together so that every block contains the "hash" (a kind of a crypted security code) of the previous one, making it almost impossible to alter the chain or otherwise abuse the transaction (see Organization for Economic Co-operation and Development – OECD 2018, 4). It is a specific technology of publicly available distributed (main) ledger: distributed ledger technology (DLT), where merging of the blocks is documented in publicly available database of unique transaction history (Jovanić 2021a, 22). Blockchain technology maybe is the most notable, but is not exclusive digital environment in which digital asset transactions are being conducted. The LDA stipulates that its provision shall apply to all digital assets and to the provision of all digital assets services referred to in the LDA regardless of the underly-

mechanism that allows the verification of transactions to be performed by the system participants themselves[8] (Radivojević 2018, 62; IMF 2016, 9). This means that there is no central authority to manage the transactions related to virtual currencies; instead, they are carried out by units simbolically called "miners",[9] who can be individuals, associations or companies, using the capacities of their own computer equipment to join the online network of the currency (Radivojević 2018, 62).

Determining the legal nature of virtual currencies is not at all a simple task. Given that they are intuitively associated with money and consequently mistakenly equated with it, in or-der to approach it in the right way, it would be useful to make a brief review of the legal nature and functions of money itself, and then compare them with the characteristics of digital assets for the sake of determining the extent to which there is an overlap.

Namely, from an economic perspective, money serves as a measure of the value of all goods, is used for payment in the circulation of any type and quantity of goods and services and enables conservation of value (Jankovec 1997, 1–2). The first-mentioned property of money cannot be attributed to virtual currencies. Natural or legal persons who accept virtual curren-cies as a means of exchange declare the price of goods and services in the national currency; how virtual currency unit will be accepted for the execution of the monetary obligation, depends on the exchange rate on the day of the transfer (in that sense Damnjanović 2022, 73). Furthermore, despite the fact that the tendency

ing technology, by which the legislator opted for the principle of technology-neutral approach (LDA, Art. 8).

[8] This does not mean, however, that the transactions related to digital assets are carried out without su-pervision. On the contrary, the LDA divided the competence in the field of digital assets between the Securities Commission (when it is about digital tokens) and the National Bank of Serbia (when it is about virtual curren-cies). Such a division of competences was made in a meaningful way, given that digital tokens represent a kind of digital counterpart of securities, while virtual currencies, although cannot be equated with money, successfully imitate, to a certain extent, at least one of its functions in the digital sense. The National Bank and the Commission shall cooperate in the performance in their respective competences. Their competences can even be intertwined in the event of so-called hybrid digital assets, which refer to digital assets that have both the features of virtual currencies and digital tokens. See the LDA, Art. 2, Para. 1. It. 4) and Art. 10, Paras. 1–4. For a detailed analysis of the supervision in the field of digital assets see Cucić 2023, 356–381.

[9] "The steady addition of a constant of amount of new coins is analogous to gold miners expending re-sources to add gold to circulation" (Nakamoto 2008, 4).

to use cryptocurrencies for the purpose of pur-chasing goods and services is increasing (Damnjanović 2022, 72–73), it remains that *de iure* it is not about payment, but exchange of virtual currencies, which means that virtual currencies do not perform the second-mentioned function of money either. Lastly, given that they are neither issued or guaranteed by a central bank or public authority (e.g., by the National Bank of Serbia or Securities Commission), their stability as a currency is questionable, because the criteria it depends on are outside the traditional monetary system, which increases the risk of unpredictable or hard-to-predict oscillations when it comes to their exchange rate. Virtual cur-rencies are, therefore, facing the volatility much higher than national currencies (IMF 2016, 17). Such an excessive volatility indicates their speculative investment purposes rather then characteristics of a currency (Yermack 2013, 16). Based on the above, it is clear that virtual currencies do not perform the mentioned functions of money; although they resemble them to a certain extent. Nevertheless, it should be kept in mind that, despite the fact that virtual curren-cies are not established as legal tender, the purchase or sale of digital assets for money is, in fact, allowed, as well as the exchange of digital assets for other digital assets (LDA, Art. 2, Para. 1, It. 7)).

1.1.2. Digital tokens

Digital token is the second type of digital assets that the LDA regulates and means any intangible property representing, in digital form, one or more property rights, which might in-clude the right of digital token user to a specific services (LDA, Art. 2, Para. 1, It. 3)). Like virtual currencies, digital to-kens do not exist in physical form. They are nothing but digital records that provide certain rights. It could be said that the term "token" is used as a "metaphor of what tokens are in phys-ical world", e.g., casino tokens, which represent value, wardrobe tokens, which grant access to another object or to a service, like telephone tokens, used for making calls from public phones (Gariddo 2023, 7). As not all digital tokens have the same function, there are several types of them that can be distinguished.

Particularly important for the titled analysis, given that their function is the same as that of traditional securities, such as bonds or shares, are security tokens (Gariddo 2023, 23). This means that the rights that these tokens symbolize are similar to or the same as the rights that are derived from securities. For instance, security tokens

promise a share in future company earnings or their owners take part of company's ownership by purchasing the tokens in a new issuance (Sovilj 2021, 303). In addition to the right of ownership, security tokens may entitle to dividend distribution (Deloitte 2020, 9) and overall grant financial benefits resulting from the issuer's main activity (Falempin et al. 2019, 6).

This raises the question of the legal relation between digital tokens and securities, i.e. financial instruments. Firstly, it should be noted that, unless otherwise provided by the LDA, the law governing the capital market[10] shall apply to the issuance of digital assets that have all the features of financial instrument and to the secondary trading and the provision of services connected with such digital assets; however, there is an exception: the law on capital market is not applicable if digital assets do not have characteristics of stocks, are not fungible with stocks and the total value of digital assets issued by a single issuer during a period of 12 months does not exceed EUR 3,000,000 in the dinar equivalent at the official middle exchange rate of the dinar against the euro determined by the National Bank of Serbia on the day of the issue, i.e. during the primary sale (LDA, Art. 7). Still, can it be said that security tokens are securities?

According to the Securities Commission (2022), the Republic of Serbia's first digital token – *Finspot factoring token* – issued by the Finspot limited liability company, seated in Belgrade, gives the right to its holder to invest in a total of four investment indices, which differ in maturity and interest rates. A token holder who has invested in one of the investment indices has the right to an interest, which is paid in dinars, at the fixed interest rate set for the selected investment index. After the index matures, the tokens that are invested return to the investor's blockchain wallet. This means that, in this case, the token legally behaves like a bond, but it seems right to conclude that it is not the same as a bond. The bonds are not among the provi-sions of the LDA. As debt securities, they are regulated by the LCM and the CA (convertible bonds). This should indicate that these are not the same legal institutes, and that the fact that a certain digital token has the features of security, i.e. financial instrument, is not enough to legal-ly equate them. In the previous example, it could be cautiously said that digital token is a kind of "digital bond", but fundamentally it remains

[10] Meaning the LCM as a current regulation in this area.

a digital token, which means that the application of the relevant provisions of the LDA cannot be avoided.

The following should be also taken into account while reaching the conclusion on this topic. Namely, the LDA seems to be quite explicit[11] regarding the rule that digital tokens repre-sent one or more *property* rights, which leaves non-property rights beyond their reach and rais-es the question of whether there is and/or should be an equals sign between the legal position of the holder of digital token (assets) on the one hand, and holders of securities that provide certain non-property rights beside the property rights, on the other. For instance, a stockholder, pursuant to his share in a joint stock company, in addition to the typical right to a share in the company's profit, has the voting right and the right to participate in the general meeting, which are classified as non-property rights. Does this mean that a digital token that, e.g., provides the right to a share in the issuer's profit, like stocks provide the right to a dividend, can be equated with such stocks, which comprise certain non-property rights as well? Viewed in this way, it appears that digital tokens, even those which have the most similarities with them, should not be equated with securities. In other words, having the features of financial instrument does not mean being a financial instrument. The provision that openned this dillema (Art. 7 of the LDA) is practically important in a different context, since it determines whether the LDA or the LCM will be applicable in a concrete case.

[11] On the contrary, on the basis of the provision that refers to the definition of digital token, a conclusion that *implicitly* follows from it can be drawn. Namely, the LDA prescribes a unique token definition, making no distinctions regarding different types of tokens, which undoubtedly exist. However, it can be noted that the first part of the provision ("... and means any intangible property representing, in digital form, one or more property rights") refers to nothing but security tokens, while the second part ("which might include the right of a digital to-ken user to specific services") refers to so-called utility tokens, which are used to access the specified services or products of the issuing company (Amroush 2022, 2). These tokens may prove to be quite useful for the com-pany's business operations, especially if the company is newly established, since it can issue tokens that give in-terested parties the right to use goods or services that the company intends to sell or provide on the market, and then, from the funds obtained from the sale of that tokens, create the necessary sources for finansing a new busi-ness venture (Mihajlović 2021b, 373). The classification of digital tokens usually also includes payment tokens (see, e.g., Garrido 2023, 20–26; Sovilj 2021, 302–303; Mihajlović 2021b, 372–373). On the other hand, given that these tokens do not provide rights, issuer claims or access to a specific product or service (Deloitte 2020, 9), it appears that they are not included in the subject provision. Considering the paper's research scope, no type of digital tokens other than security tokens will not be further discussed.

This should not affect what digital tokens (assets) and se-curities, in essence, represent, nor the rights they provide based on the laws that respectively regulate them.

2. DIGITAL ASSETS AS A CONTRIBUTION TO A COMPANY

2.1. General rules

Discussion whether digital assets can be a contribution to a company should not be brought to the table before a brief reminder of the provisions of the law that primarily regulates the subject matter, which is, of course, the CA. Understanding how this law stipulates the obli-gation to pay, i.e. enter the contribution will prove to be crucial when consindering certain types of digital assets as potential contribution to the company in question.[12]

With that being said, according to the CA, contribution to the company may be pecuni-ary or in kind, and are expressed in dinars. In kind contributions may be given in tangibles or intangibles, unless otherwise specified by the CA for certain types of companies. If a pecuniry contribution is paid in a foreign currency in accordance with the law governing foreign curren-cy operations, the dinar counter value of the contribution is calculated using the National Bank of Serbia middle exchange rate on the day of contribution payment (CA, Art. 45, Paras. 1–3). Considering these rules while keeping in mind the earlier explanations about the nature of virtual currencies and digit-al tokens, it could be said, at least at first glance, that digital assets have the potential to be le-gally eligible as a contribution to the company. Besides, this matter has also found a foothold in the LDA, which approached it from its own angle, stipulating that in kind contributions in digital tokens that are not related to providing services or execution of work are allowed, and that, notwithstanding with this rule, in kind contributions to the general or limited partnership may be in digital tokens related to providing services or execution of work (LDA, Art. 14, Paras. 2–3), correctly taking into account the corresponding exception from the CA that the partner's and

[12] There are lines in the introductory part of the paper that are dedicated to the practical importance of determining the contribution of each company member; see n. 2.

general partner's in kind contribution may consist of providing services or execution of work (CA, Art. 96, Para. 2 and Art. 129, Para. 1). The list of digital tokens that the LDA refers to when stipulating that in kind contributions in digital tokens are allowed shall be established by the Securities Commission (LDA, Art. 14, Para. 4).

It is different with virtual currencies. As previously explained, unlike digital tokens, virtual currencies do not symbolize any property right that could be entered as an in kind contri-bution to the company. The purpose for which virtual currencies are used does not derive its value from any rights; they are used solely as a means of exchange. Once again, it is important to underline that, since virtual currencies do not have the legal status of money or a currency, and their issuance and overall use rest on a system that differs and is separate from the tradition-al monetary system, they are not eligible to be a pecuniary contribution to the company either, at least not in their original form. Namely, virtual currencies may be converted (exchanged) for money and then paid into a company as a contribution in money (LDA, Art. 14, Para. 1). Nevertheless, this still does not mean that virtual currencies are contribution to the company. It is important to be precise and notice that what actually becomes a contribution are not virtual currencies, but the money obtained by exchanging virtual currencies for it. Therefore, after the conversion of virtual cur-rencies, the matter continues to follow the rules that apply to pecuniary contributions in the sense of the CA as the "parent" law of this issue.

2.2. Appraisal of digital tokens as an in kind contribution

Appraisal of in kind contributions is quite an important task: the company's share capi-tal represents the *pecuniary* value of the company's members' contributions (CA, Art. 44, Para. 3), meaning both pecuniary and in kind. The company's members acquire a share in the company proportionately to the value of their contribution into the company's share capital, unless otherwise provided by the memorandum of association upon company incorporation or by a unanimous resolution of the general meeting (CA, Art. 151, Para. 1). The principle of maintaining the value of the company's share capital acts as general "pledge" to secure the company's creditors (Vasiljević 2013, 108), which can also be said for the need to realistically present the value of the company's share capital. If it is not presented in such a way as to

correspond to the true state, either intentionally or uninten-tionally, third parties as potential creditors of the company could be misled regarding the com-pany's ability to repay its eventual debts.

When it comes to digital tokens, the appraisal needs to be adjusted to their legal features. Therefore, the question arises as to how it will be implemented. The LDA does not address this issue; the procedure and conditions of appraisal of in kind contributions is regulated by the CA, and it should be considered whether its provisions in this matter are applicable in the event of appraisal of digital tokens.

According to the CA, in kind contributions to the company are appraised by a certified expert witness, auditor or other qualified person authorized by a competent state authority of the Republic of Serbia to appraise the values of certain tangibles and intangibles. The appraisal may also be performed by a company that meets the conditions prescribed by law to appraise the value of tangibles and intagibles subject to appraisal (CA, Art. 51, Paras. 1–2). There appears to be no obstacle to the application of this provision to the appraisal of digital tokens as well (when they are used as an in kind contribution). Primarily, the provision emphasizes the appraiser's expertise and authorized position. These conditions are undoubtedly among the most important ones that must be met in order for the appraisal to be valid. Furthermore, the appraiser is appointed to appraise the values of *certain* tangibles and intangibles, which may be understood as the need to appoint a natural or legal person with appropriate qualifications for the appraisal of a specific type of right provided by the token in question. Taking into account the previous explanations regarding digital tokens, it seems justified to conclude that the subject of the appraisal is not the token as such, but one or more property rights incorporated into it. A token is nothing more than a digital record on a corresponding digital ledger technology. Digital tokens derive their value from the right(s) they represent, which means that the nature of that right should de-termine the direction of appraisal. Accordingly, the appraisal includes in particular: (1) descrip-tion of each tangible or intangible constituting the in kind contribution; (2) appraisal methods used and (3) the statement as to whether the appraised value is at least equal to par value of the shares acquired in the case of a general partnership, limited partnership and a limited liability company or par value of the stock acquired, or accounting value in the case of stocks without par value, increased for the premium paid for such stocks if it exist, in the case of a joint stock company (CA, Art. 52).

The situation is somewhat more complex in "borderline" cases. Those cases imply digit-al assets that have the features of both digital tokens and virtual currencies, i.e. digital assets that not only provide certain rights, but can be used as a means of exchange at the same time (hybrid digital assets). As previously stated, the only option for virtual currencies to find their way into the company is to be converted into money and then as money, as a pecuniary contri-bution, be paid to the company. Therefore, it is a situation in which the potential contribution to the company is both in kind and pecuniary (provided that the conversion has been conduct-ed). How should the appraisal be carried out in that case? Neither the LDA nor the CA do not (directly) regulate this issue; the solution must be found on the ground of already existing rules.

Additionally, there is no clear answer to the question of whether a general manager, board of directors/supervisory board if management of the company is organized in two-tiers should be allowed the freedom to choose the appraiser if digital tokens are the ones that should be appraised (CA, Art. 53). Namely, guided by what criteria the company's management should make the choice of the appraiser, especially if it is not competent enough in terms of digital assets. Considering that digital assets have been given a special attention by passing the law entirely devoted to them, it is clear that digital assets consitute a delicate legal area that is minimally tolerant of mistakes and and any kind of abuses. In that spirit, it seems that it would be useful to prescribe in the form of a non-*numerus clausus* list of criteria by which the management of the company should be guided while selecting the appraiser. In any event, if it is opted for the application of the provision of the CA that refers to the conditions that the appraiser must meet (Art. 51, Para. 1 – criterion of expertise and authorised position), that provision should be understood as "the first line of defense" against possible abuses, while the list of guiding criteria should provide additional legal certainty and further reduce the chances of abuse.

3. DIVIDEND IN THE FORM OF DIGITAL ASSETS

As previously discussed, digital assets, or to be more precise, digital tokens, may entitle its holder to dividend distribution. This should not be confused with the dilemma of whether the company's profit – a dividend – can be paid to the company's members in the form of digital assets. The right to a dividend is one of the basic property rights of

a shareholder. According to the CA, a dividend may be paid in cash or company stocks, pursuant to the resolution on payment of dividend. If dividends are paid in the form of stocks of the company, such a payment shall be approved by the stockholders of the class of stocks to which such a payment is made under the rules on voting of stockholders within a class of stocks and payment to each stockholder of a class of stocks who is entitled to dividend is made in stocks of that class (CA, Art. 272, Paras. 1–2). This means that the CA has limited the methods of dividend payment, without the possibility to add new ones. Is there a basis for dividend payment in any of the forms of digital assets?

In the introductory part of the paper, is it underlined that virtual currencies are not mon-ey, regardless of the fact that they are accepted by natural or legal persons as a means of ex-change. Therefore, even if there was a stockholder's consent for a dividend to be paid to him in the form of virtual currencies, such a payment would not be in accordance with the rule on the methods of dividend payment. On the other hand, there are digital tokens that may have the features of financial instrument, in this case – stocks. If dividends are paid in the form of the company's stocks, it should be added to the abovementioned rules that a dividend may be paid in the form of stocks of some other type or class only if any such a payment is approved by a three-quarter majority of the present stockholders holding the stocks of the class of stock to which such a payment is made and by the same majority of votes of the stockholders of the class of stock in whose stocks the dividend is paid (CA, Art. 272, Para. 3).

In other words, the payment of dividends in the form of stocks of the company is subject to a number of rules that need to be determined as to whether they can be applied to such to-kens. Seemingly, it is not clear how these requirements would be complied with if the dividend was intended to be paid in digital tokens. Digital tokens represent various rights against a com-pany, similar to how different classes of stocks provide different stockholders' rights. However, analogously applying the rules regarding the payment of dividend in the form of the company's stocks in the event of digital tokens as a potential payment method appears difficult to imple-ment. Perhaps a dividend payment in the form of digital tokens would be possible in an ideal scenario in which all the company's members participate in its share capital in digital tokens that could be classified into classes in the same way as is done with stocks. Although, even if that scenario were to come true,

the question is whether there would be any talk of a joint stock company at all: a joint stock company is a company whose share capital is divided in stocks (not tokens) held by one or more stockholders (CA, Art. 245, Para. 1). With all of that being said, the law does not seem to leave room for a dividend to be paid to stockholders in any form of digital assets.

4. DIGITAL ASSET SERVICES AND COMPANIES

A significant part of the LDA is dedicated to regulating the provision of digital asset services. In the subsequent lines, it will be explained what these services comprise, who is au-thorized to provide them and under what conditions, followed by appropriate observations.

4.1. Types of digital asset services

Digital asset services are various and include: (1) reception, transmission and execution of orders relating to the purchase and sale of digital assets on behalf of third parties; (2) pur-chase and sale of digital assets for cash and/or scriptural money and/or e-money; (3) exchange of digital assets for other digital assets; (4) custody (safekeeping) and administration of digital assets on behalf of digital asset users and the related services; (5) services pertaining to the is-suing, offering and placing of digital assets on a firm commitment basis (underwriting) or with-out a firm commitment basis (uncommitted placement/ agent services); (6) maintaining a regis-ter of pledges on digital assets; (7) digital assets acceptance/transfer services; (8) digital asset portfolio management and (9) operation of a digital assets trading platform (LDA, Art. 3, Para. 1, Its. 1) to 9)).

Certain similarities can be found between the services pertaining to the issuing, offering and placing of digital assets on a firm commitment basis or without a firm commitment basis and the process of issuing securities. Namely, in the latter, the issuer can hire a person who will help in the activities related to the emission in question. That "person" is actually an investment company, which either carries out operations pertaining to the offering and placing of the secu-rities on a firm commitment basis, which is classified as underwriting, or without a firm com-mitment basis, which is understood as agent services

(Jovanović, Radović, Radović 2021, 452–453). The difference between the two variants lies, therefore, in the scope of obligations related to the activities in question.

Digital asset services can also be of an advisory nature. In that event, they include the provision of investment advice, investment recommendations, advice on capital structure, busi-ness strategy, issuing of digital assets and similar, as well as other digital asset advisory servic-es. Apparently, a distinction between investment advice and investment recommendation is made. Investment advice means the provision of personal recommendations to a user of digital assets, in respect of one or more transactions relating to digital assets, while investment recom-mendation means investment research or other information for the public that explicitly or tacit-ly recommends or suggests an investment strategy regarding digital assets (LDA, Art. 5).

4.2. Digital asset service providers

4.2.1. Legal form

In terms of the LDA, digital asset service provider means a legal person providing one or more services in connection with digital assets (LDA, Art. 2, Para. 1, It. 5). The definition is specified by the provision that stipulates that a digital asset service provider shall have the legal form of a company within the meaning of the governing companies (LDA, Art. 51). As when defining digital token, the LDA did not take into account that there are different types of digital asset services, thus prescribing a single concept of digital asset service provider, as explained just before. Nevertheless, there are several bylaws adopted on the basis of the LDA that nuance the Law's provisions.

For instance, the Decision on Detailed Conditions and Manner of Supervision over Vir-tual Currency Service Providers and Virtual Currency Issuers and Holders stipulates that, for the purposes of this Decision, "service provider" means a digital asset service provider in the part of its operations pertaining to virtual currencies that is a company licensed by the National Bank of Serbia to provide virtual currency services.[13] There is also the Decision on the Content of the Register of Virtual Currency Service Providers and Detailed Condi-

[13] Decision on Detailed Conditions and Manner of Supervision over Virtual Currency Service Providers and Virtual Currency Issuers and Holders, *Official Gazette of the RS,* 49/2021, Para. 2, It. 1).

tions and Manner of Keeping that Register, which prescribes that, e.g., the register number of the service provider, its business name and head office address and the number and date of the National Bank of Serbia's decision licensing the service provider for the provision of virtual currency services, as well as the number and date of all National Bank of Serbia's decisions amending or supple-menting that licence shall be entered in the Register of virtual currency service providers.[14]

The stated examples of bylaws are intended to support the position that the provisions of the LDA are not isolated, and, as is practically the case with every law, that they are elaborat-ed and clarified by various bylaws adopted on the basis of it. In addition, two important details can be observed from the cited provisions. The first is that the service provider shall have the legal form of either a general partnership, limited partnership, limited liability company or a joint stock company (CA, Art. 8). An enterpreneur, accordingly, is not allowed to provide digital asset ser-vices. However, an advisory service provider shall have the legal form of a company *or* entrepreneur *or* be registered as a natural person performing a free profession as an activity in accordance with separate regulations (LDA, Art. 55, Para. 3, emphasis added), meaning that, when it comes to ser-vices of an advisory nature, the requirement regarding the legal form is, justifiably, *lighter* than regarding digital asset services that do not have such a nature, taking into account the risks as-sociated with performing them respectively. The second is that the company must be licenced in order to provide digital asset services. The obligation to obtain the licence and its practical significance are considered in more detail as a subtopic below.

4.2.2. Minimum capital

The same amount of minimum capital is not required for every legal form of a company.

When it comes to limited liability company, the minimum capital is symbolic and amounts to at least RSD 100 (CA, Art. 145).[15] For joint stock companies, the minimum capital is significantly higher and amounts to at least RSD 3,000,000 (CA, Art. 293). High minimum

[14] Decision on the Content of the Register of Virtual Currency Service Providers and Detailed Conditions and Manner of Keeping that Register, *Official Gazette of the RS*, 49/2021, Para. 3, Its. 1) to 2) and It. 4).

[15] About the reasons why the lower limit of the minimum share capital in the event of this legal form is set to this low, see Jovanović, Radović, Radović 2021, 370.

share capital requirements should act as deterrent to small investors (Jovanović, Radović, Radović 2021, 455), i.e. as a threshold that only those investors who intend to sustainably engage in the chosen activity (business opera-tion) are willing to cross, under the assumption that the payment of the required amount is a signal of a planned and potentially successful business venture.

It should be noted that the rules regarding the minimum capital of a limited liability company and joint stock company are subject to suspension, in the event that a higher amount of minimum capital is prescribed by a special law for companies dealing in certain business activities (CA, Art. 145 and Art. 293). In the context of this analysis, that special law is the LDA, which prescribes the minimum capital of the company submitting the application for a licence to provide digital as-set services.

If the company intends to provide digital asset services referred to in Art. 3, Para. 1, Its. 1) to 6) of the LDA, the minimum capital shall be no less than EUR 20,000 in the dinar equiva-lent at the official middle exchange rate of the dinar against the euro determined by the National Bank of Serbia; for providing digital asset services referred to in Its. 7) and 8), no less than EUR 50,000, and if the company intends to operate a digital assets trading platform, the min-imum capital required amounts to EUR 125,000. Notwithstanding, if the company intends to operate a platform for trading in digital tokens of a single issuer, its minimum capital shall be no less than EUR 20,000 in the dinar equivalent at the official middle exchange rate of the dinar against the euro determined by the National Bank of Serbia (LDA, Art. 54, Para. 1, Its. 1) to 3) and Para. 2). If a company applying for a licence to provide virtual currency services intends to provide virtual currency services for which different amounts of the minimum capital have been prescribed, it must have minimum capital in the amount prescribed only for the virtual currency service or services for which the highest amount of the minimum capital has been prescribed.[16]

It is noticeable that the highest amount of minimum capital is required for the operation of a digital assets trading platform, which is understandable, given that by obtaining a licence to provide the mentioned service, the service provider performs, as the platform

[16] Decision on the Manner of Calculating the Minimum Capital and Reporting on Minimum Capital of a Virtual Currency Service Provider, *Official Gazette of the RS,* 49/2021, Para. 2, It. 4.

organizer, complex tasks that arise from the properties of the platform, through which companies that have the permission of the supervisory authority to provide digital asset services, as well as all other legal and natural persons and enterpreneurs, can trade in the Republic of Serbia (Mihailo-vić, Danilović Terzić 2022a, 114; see LDA, Art. 30).

As can be seen, for the majority of digital asset services, the LDA does not prescribe the amount of minimum capital higher than that required as a minimum for joint stock compa-nies. When a higher amount is indeed required, it is due to the nature of the service to be provid-ed, given that the provision of such services is accompanied by greater formalities and risks[17] (as is the case with the operation of a digital assets trading platform) which, consequently, af-fects the amount of minimum share capital required from the company-service provider.

4.2.3. License application

A company intending to provide digital asset services shall submit to the supervisory authority an application for a licence to provide digital asset services (LDA, Art. 56, Para. 1). The list of data to be submitted with this application is quite extensive, which should not be suprising considering the specifics involved in providing digital asset services and the complexity of digital assets in general. It could be said that the LDA paid special attention to the conditions that imply long-term planning of certain aspects of digital asset service providing, by which the company should "convince" the supervisory authority of the stability of its intended business operations and to make a positive decision upon its request.

In that sense, the company-applicant must support its application by the business plan with revenue and expenditure projection for the period of the first three years of operation, based on which it is possible to conclude that the applicant will be capable of meeting adequate organisational, personnel, technical and other conditions for continuous, safe and sound opera-tion, including the number and type of expected digital asset users, and the expected volume and amount of digital asset transactions, for each type of service connected with digi-

[17] The very nature of these services and risks that they carry implies the application of a stricter legal re-gime than the one that is applied in accordance with the law governing companies. These are the subjects whose regulation requires a special legal framework of business operations (Mihailović, Danilović Terzić 2022b, 158).

tal assets it intends to provide. Additionaly, the company is expected to provide the supervisory authority with the: (a) description of the planned staff training programme in connection with digital as-set transactions; (b) description of the organisational structure, including data on the planned outsourcing of some operational tasks relating to the provision of digital asset services; (c) de-scription of planned measures for managing the security of the information and communications system, as well as a number of data that indicates that the company's personnel have a good business operation (LDA, Art. 56, Para. 2, It. 5) and Its. 9) to 17)). With that being said, it is safe to conclude that the company is ex-pected to show a certain/high degree of responsibility already through the application, in terms of three very important aspects of digital asset service providing: personnel, structural and se-curity system. By putting the provision of digital asset services under the permit regime, a big step has been taken in the direction of creating the legal certainty regarding the conduct of dig-ital asset services and business operations of their providers (Mihailović, Danilović Terzić 2022b, 158–159).

5. FINAL REMARKS

Digital assets represent a relatively young, but without any doubt, increasingly topical subject of legal interest, which is yet to experience its full momentum. By passing the LDA, the Republic of Serbia opened its door to a new type of investment-attractive market and inova-tive business ventures it offers. A special role in that market belongs to companies, which, as it was discussed, claimed the role of digital asset service providers. Especially in the context of digital tokens, it becomes easier for startup companies to raise capital needed to support their business operations.

The conducted analysis is based on the laws that, seemingly, have nothing or little in common; it turned out, as a matter of fact, that the LDA and the CA are intertwined regarding quite a few issues, and that it is often not enough to rely on the provisions of only one of them, without consulting the other.

As it could be concluded, digital assets a potential contribution to a company must be considered from the CA's point of view as well, given that this law prescribes the types of con-tributions and regulates

the procedure of appraisal of in kind contribution, under which catego-ry digital tokens fall according to the LDA. While the only way for virtual currencies to become a contribution to a company is to be converted into money and then payed to the company in question in the pecuniary form, there is no clear answer on how to approach the problem of hy-brid digital assets as a potential contribution, i.e. their appraisal as such. The solution could be to appraise the value of the rights that such assets confer and to add to it an estimated value of their potential to be used as a means of exchange (in essence, to approach the problem in the same way as is done with regular in kind contribution). If at the moment when hybrid digital assets are to be appraised their exchange possibility has already been exhausted and such assets have already been ex-changed for money, there is no obstacle to treat such assets as a pecuniary contribution in the way described above.

Several observations can be made when it comes to the minimum share capital of the companies that intend to provide digital asset services. Primarily, the lower limit of the mini-mum capital is not excessively high for majority of digital asset services. That circumstance might be understood as a consequence of the legislator's desire to encourage a greater number of potential applicants willing to enter this perspective new market. If it was the opposite, if the minimum share capital requirements were disproportionately high in the eventual aspiration to tighten the regulation of digital assets and allow entry to the new market only to those partici-pants who, based on the high capital they are ready to invest, send a signal that they expectedly will be sustainable by operating within its framework, chances are good that a certain number of possible digital asset service providers would be, at the very begining, deterred of this type of business operations. Ensuring that only the most sustainable and promising participants se-cure their entry to the market of digital asset service providing does not depend only on seting a high minimum share capital limit, but on prescribing other, more or less strict conditions that companies-applicants must meet. As could be seen, the LDA indeed precribes and regulates in detail such additional conditions. In other words, it can be said that a legislator made a good choice by prescribing the minimum share capital requirements in the way explained above.

Finally, it is safe to say that digital assets have enormous practical potential in the light of companies' business operations. The challenges that digital era brings are constantly becom-ing more complex,

thereby expanding the possibilities in terms of practical activities related to digital assets. Based on everything previously stated, the conclusion is that the foundation of issues considered in this paper is well laid, but that their further "construction" should be even more detailed than it is now. In any event, it remains to be seen how these issues will be re-solved in practice and whether (and it is practically certain they will), new ones will appear, requiring additional considerations and creative problem-solving approaches.

REFERENCE LIST

1. Amroush, Fadi. 2022. Tokenizing Startups, from Utility Tokens into Security Tokens. *https://mpra.ub.uni-muenchen.de/116021/1/MPRA_paper_116021.pdf*, last visited 28 October, 2023.
2. Cucić, Vuk. 2/2023. Nadzor u oblasti digitalne imovine. *Pravo i privreda* 61: 356–381.
3. Damnjanović, Nikolija. 2022. Pravna priroda kriptovaluta. *Harmonius, Journal of Legal and Social Studies in South East Europe* 6: 71–96.
4. Deloitte. 2020. Are Token Assets the Securities of Tommorow? *https://www2.deloitte.com/content/dam/Deloitte/lu/Documents/technology/lu-are-token-assets-the-securities-tomorrow.pdf*, last visited 28 October, 2023.
5. International Monetary Fund. 2016. Virtual Currencies and Beyond: Initial Considera-tions. *https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf*, last visited 28 October, 2023.
6. Falempin, Luc, Philippe Van Hecke, Daniel Coheur, Eamon Walsh. 2019. Tokenized Securities. The Ultimate Handbook on how to Issue Compliant Securities on the Blockchain. *https://tokeny.com/wp-content/uploads/2019/01/TOKENIZED-SECURITIES.pdf*, last visited 28 October, 2023.
7. Gariddo, José M. 2023. Digital Tokens: A Legal Perspective. International Monetary Fund. *https://www.imf.org/en/Publications/WP/Issues/2023/07/28/Digital-Tokens-A-Legal-Perspective-537041*, last visited 28 October, 2023.
8. Huang, R. H., Demin Yang, Ferdinand Fai Yang Loo. 2020. The Development and Regulation of Cryptoassets: Hong Kong Experiences and a Comparative Analysis. *European Business Organization Law Review* 21: 319–347.
9. Jankovec, Ivica. 11–12/1997. Pravni pojam novca. *Pravo i privreda* 34: 1–10.
10. Jovanić, Tatjana. 2021a. Kripto-imovina kao primer uticaja digitalizacije na pravo i praksu regulatornih organa. *Međunarodna naučna konferencija "Pravo i digitalizacija", Zbornik radova*: 21–39.

11. Jovanić, Tatjana. 2021b. Kriptovalute kao novi izazov zaštite potrošača. *Zaštita kolektivnih interesa potrošača, Međunarodna naučna konferencija, Zbornik radova*: 396–427.
12. Jovanović, Nebojša, Vuk Radović, Mirjana Radović. 2021. *Kompanijsko pravo, Pravo privrednih subjekata. 2nd edition*. Belgrade: University od Belgrade – Faculty of Law.
13. Mihailović Jovana, Ivana Terzić Danilović. 1/2022. Pružaoci usluga povezanih s virtuel-nim valutama – pojedini statusnopravni aspekti. *Pravo i privreda* 60: 138–160.
14. Mihailović Jovana, Ivana Terzić Danilović. 2022. Osobenosti poslovanja pružalaca usluga povezanih sa virtuelnim valutama kroz prizmu njihovu delatnosti. *Zbornik radova sa XXX Susreta pravnika u privredi Srbije*: 108–131.
15. Mihajlović, Borko. 2021a. Digitalna imovina u pravnom sistemu Srbije: osnovne karakte-ristike. *Usklađivanje pravnog sistema Srbije sa standardima Evropske unije*: 595–609.
16. Mihajlović, Borko. 2021b. Zaštita potrošača na tržištu digitalne imovine. *XXI vek – vek usluga i uslužnog prava*: 369–381.
17. Motika, Željka. 1/2022. How Digital is the New Serbian Law on Digital Assets? *Pravni zapisi* 13: 93–112.
18. Motika, Željka. 2021. ICO u Srbiji – Izdavanje digitalne imovine po Zakonu o digitalnoj imovini. *https://lawlife.rs/index.php/pravo/178-ico-u-srbiji-izdavanje-digitalne imovine-po-zakonu-o-digitalnoj-imovini*, last visited 22 January, 2024.
19. Nakamoto, Satoshi. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. *https://bitcoin.org/bitcoin.pdf*, last visited 22 January, 2024.
20. Organization for Economic Co-operation and Development, OECD Blockchain Primer. *https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf*, last visited 28 October, 2023.
21. Radivojević, Aleksandar. 2018. Virtuelne valute, razvoj i regulacija. *Ekonomske ideje i praksa* 29: 59–71. *https://www.ekof.bg.ac.rs/wp-content/uploads/2014/10/Rad-04.pdf*
22. Securities Commission. 2022. *https://www.sec.gov.rs/index.php/en/news/actual/775-commission-approves-issuance-of-the-first-digital-token*, last visited 28 October, 2023.
23. Sovilj, Ranko P. 1/2023. Similarities and differences in the issuance of securities and digit-al assets – the issue of legal responsibility of the issuer. Glasnik *of the Bar Association of Vojvodina* 95: 196–233. *https://scindeks.ceon.rs/article.aspx?artid=0017–09332301196S*
24. Sovilj, Ranko P. 2021. Legal Aspects of Digital Asset Market in the Republic of Serbia. *Collection of papers from the second International Scientific Conference Regional Law Review*. 297–311.

25. Vasiljević, Mirko S. 2013. *Korporativno upravljanje – izabrane teme*. Belgrade: The Busi-ness Lawyers Association of the Republic of Serbia.
26. Vasiljević, Mirko S. 2019. *Kompanijsko pravo, Pravo privrednih društava. 11th edition.* Belgrade: University of Belgrade – Faculty of Law.
27. Vujović, Bogdan. 1–6/2023. Regulativa digitalne imovine u Srbiji – propuštena prilika za razvoj tržišta ili neiskorišćeni potencijal. *Finansije* 78: 75–95.
28. Yermack, David. 2013. Is Bitcoin a Real Currency? An Economic Appraisal. NBER Working Paper Series. *https://www.nber.org/system/files/working_papers/w19747/w19747.pdf*, last visited 28 October, 2023.

UDK 341.322-056.26:004:376
DOI 10.51204/IVRS_24103A

Sofija Lekić*

THE IMPACT OF DIGITAL TECHNOLOGIES ON THE CULTURAL RIGHTS OF D/DEAF AND HARD-OF-HEARING PEOPLE

Digital technologies permeate almost all spheres of human lives in contemporary times, affecting a number of aspects of people's lives. Such is the case with cultural rights as well, especially in the cases of certain groups. The paper is focused on the impact of digital technologies on these rights of d/Deaf and hard-of-hearing people. The theoretical framework of the paper defines the concepts of culture and general and specific cultural rights, as well as the labels of deaf, Deaf and hard-of-hearing. Then, an overview of relevant digital technologies is provided, with an evaluation of the impact they have on these cultural rights. Finally, possible strategies for improvement are broadly defined, and a conclusion is provided, summarizing the results of the research done.

Key words: *assistive technologies, cultural rights, Deafness, Deaf studies, digital technologies*

1. INTRODUCTION

During the last few decades, the world has borne witness to an incredible growth in the diversity and ubiquity of digital technologies, both those reserved to only certain groups of people and those available to the general public. Consequently, the impact of said technologies on the many areas of people's lives has broadened and intensified, making it an important subject to study and analyze. Among the many questions raised in relation to this, the impact of digital technologies on human rights has been one of those which attracted the most attention. In relation to this paper, the main topic addressed are the rights of d/Deaf and hard-of-hearing people – precisely, their cultural rights.

* The author is an undergraduate student at the University of Belgrade – Faculty of Law and University of Belgrade – Faculty of Political Sciences, *sofia1054sofia@gmail.com*.

The paper is divided into three general, overarching sections. Firstly, the broad concept of cultural rights is examined. Attention is devoted to a number of different cultural rights, as well as the very concept of culture and its relation to some of the rights mentioned. Next, a section deals with the differences between the three labels concerning the group of people whose cultural rights are examined in the paper – the deaf, Deaf and hard-of-hearing people. Lastly, the third general section concerns digital technologies affecting the cultural rights of d/Deaf and hard-of-hearing people. A general overview of the most prominent technologies concerning this topic is given, and then an analysis of their effects on the cultural rights of d/Deaf and hard-of-hearing people is provided.

In the end, attention is drawn to the benefits provided by these digital technologies, as well as the main issues they cause in relation to the cultural rights of d/Deaf and hard-of-hearing people. The aim of the conclusion is to provide an evaluation of the current situation concerning the topic at hand, but also to give guidance for the future period, so that the power of digital technologies keeps on being harvested in the service of improving the cultural rights of d/Deaf and hard-of-hearing people, while being as little of a detriment to them as possible.

2. CULTURE AND CULTURAL RIGHTS

2.1. The General Concept of Culture

The exploration of the titular topic of the paper demands the provision of a solid theoretical framework preceding the examination of the practical aspects of the question posed. The concept of cultural rights, which is arguably the very core of the issue at hand, appears to be the most suitable starting point for this – nevertheless, its definition cannot be ascertained without first devoting attention to the concept of culture itself. Thus, it is necessary to consult a body of different conceptions of culture, in order to provide a well-rounded, multifaceted understanding of its meaning.

A broad idea of the concept may be found in its understanding as "[t]he product of the man, created through history and made by a row of previous generations, which every new generation adopts and adapts" (Stojković 1999, 36). However, the true meaning of the term

cannot be reached through the analysis of this definition alone; its complex nature dictates the existence of a plethora of its perceptions, making it necessary to consult some of the more elaborate definitions in order to gain a true understanding of its scope and variability.

The first question to be posed may be that of the justifiability of using the term "culture" with the intention and understanding of it signifying a single material concept. In effect, while "one widely accepted proposition is that there exists a 'universal' culture and that, while some people are able to enjoy it, others may not have access to it [...] [another interpretation defines culture as a] group's own culture, and not necessarily [...] some general or supposedly universal culture, because these two concepts are not necessarily coterminous" (Stavenhagen 2001, 88). As will be shown later on, when discussing the concept of cultural rights, the distinction between the subjects of the rights being defined as members of humankind on the whole, as opposed to their identification as members of a certain group, demands the taking into account of these differing views of the concept of culture in general.

The two conceptions of culture shown above have a significant impact on the importance of defining culture in a precise way, when it comes to the definition of cultural rights. Should the concept of one, "universal" culture be adopted, the cultural rights a person is guaranteed would be supposedly available and identical in their content to everyone. Also, the nature of the rights would be almost entirely individualistic – culture itself would be regarded as an abstract, overarching phenomenon, or a sort of a public good, which then every person would be entitled to. Yet, regarded through the prism of culture being understood as pertaining to a certain group, cultural rights become more of a communal concept, tied to the group as a social unit. Their content, thus, is not the same for all people; rather, a person's status as a subject of a certain cultural right is dependent on their belonging to a group which "owns" the culture in question.

Regardless of the singularity and/or plurality of culture as a phenomenon, its structure is complex and susceptible to different interpretations. One of these is provided by Rodolfo Stavenhagen, who recognizes three different aspects of the concept of culture: culture as capital – the "accumulated material heritage"; culture as creativity – "the process of artistic and scientific creation"; and culture as a total way of life – "the sum total of the material and spiritual activities and

products of a given social group which distinguishes it from other similar groups" (Stavenhagen 2001, 87–89). On the other hand, Pok Yin Stephenson Chow recognizes four different meanings of culture – culture as high culture, culture as popular culture, culture as a way of life, and culture as sets of collective memories – that is, "the aspect of culture that consists of shared ideas and beliefs of history, ancestry and of life sustained in a community of individuals' memory, lived, signified, expressed and enacted, which gives heritage and cultural practices their meaning" (Chow 2014, 613–614).

However, as much as all these understandings of the meaning of culture are important for the overall understanding of the general concept of culture, it may be argued that the crucial one for the purposes of this paper is the understanding of culture as a way of life. Its relevance in defining the concept of culture may be deduced from its being the common denominator between the two previously shown categorizations of the aspects of culture (Stavenhagen's and Chow's). As has been mentioned, this is the understanding of culture which sees it as a way of distinguishing groups among each other; at the same time, it may be said that culture as a way of life "is central to an expression of the identity of an individual or a community" (Ssenyonjo 2016, 627), which makes this definition the most relevant for the topic at hand.

2.2 The General Concept of Cultural Rights

The concept of cultural rights is one often mentioned in public discourse, yet also often overlooked when it comes to the practical work done in the service of the overall human rights protection. Generally speaking, cultural rights are classified as second generation rights, along with economic and social rights. Still, more often than not, economic and social rights get way more attention than cultural rights do.

The meaning of human rights is not an objective fact – rather, their meaning stems from certain social norms and understandings, typical for the time and place at which the rights are considered and/or provided. This comes from the fact that "[a]ll legal rights are social constructs, the product of social struggle" (Woods 2005, 128) – therefore, their content depends on the interpretation of relevant actors, which makes understanding them in a definite way nigh impossible.

Nevertheless, a general understanding of their nature can be achieved, which will be sufficient for the evaluation of the topic at hand.

Following the already mentioned fact that human rights are social constructs, it is evident that different human rights are related to each other, and not existent as separate entities. This is especially true for cultural rights, whose scope is often difficult to define in a way precise enough to deal only with the legal rights concerning culture (and not with other aspects of culture in general), yet broad enough to encompass all the ways in which legislation (domestic or international) provides people with protection for their cultural lives. In order to do so, it is necessary to recognize that "cultural rights are closely related to other individual rights and fundamental freedoms such as the freedom of expression, freedom of religion and belief, freedom of association, and the right to education" (Stavenhagen 2001, 85).

Seeing as, compared to other human rights of the first and second generation, cultural rights are often overlooked or not examined in enough detail, it comes as no surprise that there is often a lack of consensus on their content, as well as their enforceability and obligatory nature. They are often considered a controversial area (Smith 2007, 30), while their judicial enforcement is said to be "an inherently flawed and inadequate enterprise" (Woods 2005, 128).

When it comes to the examination of the general concept of cultural rights, the most important issue to be raised is that of the subjects whom they protect. In effect, a question can be posed

> "whether the concept of cultural rights can be adequately encompassed by a notion of universal individual rights, or whether they should be complemented by a different approach: that of collective or communitarian rights [...] [since] some of these rights can only be enjoyed by individuals in community with others and such a community must have the possibility to preserve, protect and develop its common culture" (Stavenhagen 2001, 92).

The issue raised here once again calls attention to the rift between singularism and pluralism in the approach to defining culture. The notion of universal individual rights is mostly suited to the concept of culture as a singular phenomenon, common to all people; on the other hand, defining cultural rights as collective or communitarian rights keeps in line with the pluralist understanding of culture as pertaining to a specific group of people.

2.3. Specific Cultural Rights

Having provided a framework for defining the concepts of culture and cultural rights in their general sense, attention is now redirected to the examination of different specific cultural rights. The starting point for this is found in the International Covenant on Economic, Social and Cultural Rights (ICESCR 1966), as the most widely recognized and most thorough legal source on protection of cultural rights in the international legal system. However, the scope of the paper in this regard surpasses the norms of the ICESCR, taking into account other relevant sources of international law in this area, as well as the academic works concerning this topic. Thus, a catalogue of specific cultural rights is devised for the purposes of the paper, comprised of the following rights: right to education, right to take part in cultural life, right to enjoy the benefits of scientific progress and its applications, right to culture, protection of cultural heritage and language (linguistic) rights.

The first cultural right provided for by the ICESCR, and one of the most developed specific cultural rights on the whole, is the right to education (art. 13–14). It is "entrenched as a fundamental human right at international, regional and national levels [...] [and] has become increasingly central to the broader human rights framework as a widely recognized 'empowerment' right" (Veriava, Paterson 2020, 113). The relevance of this right is also confirmed through the General Comment No. 13 of the UN Committee for Economic, Social and Cultural Rights (CESCR), which elaborates further on its content (CESCR 1999). The high level of development of this right is largely due to the fact that it is not solely related to culture and cultural rights – on the contrary, its relevance is also reflected in its role in the provision of necessary conditions for the future realization of other human rights, such as economic and social rights (e.g. through gaining the necessary education for future employment), which gives them an added importance in the eyes of the relevant actors working on their development and protection.

Other than the right to education, the ICESCR also provides for the right to take part in cultural life (art. 15.1.b). Once again, the CESCR produced a General Comment on the right, providing a more thorough examination of its components and overall meaning (CESCR 2009). Thus, three aspects of the right are recognized – participation

in, access to and contribution to cultural life. Such an operationalization provides the subjects of this right with a range of degrees of interaction with cultural life – a person may simply consume the contents of cultural life (access it), share the experience with other subjects (participate in it), or create new content to become part of it (contribute to it). Through its examination, at the same time, it is possible to observe the evolution of the right through time – for comparison's sake, the Universal Declaration of Human Rights (UDHR) only guaranteed the right "to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits" (UDHR 1948, art. 27.1), which is much less than the current level of development of this right.

Alongside these, a guarantee is provided by the ICESCR for the right to enjoy the benefits of scientific progress and its applications (art. 15.1.c), which can be further defined as being comprised of four elements: access to the benefits of science; contribution to science; participation in decision-making concerning science; and conservation, development and diffusion of science and culture (Ssenyonjo 2016, 637). As will be further elaborated in the following parts of the paper, when it comes to the topic discussed, the most relevant aspects out of the mentioned four are the access to the benefits of science and the participation in decision-making concerning science.

However, not all cultural rights are mentioned in the highest instruments of international law, such as those previously mentioned. Still, that does not make them any less worthy of the label of cultural rights – only less protected in a judicial sense. These rights are most often examined in theoretical and academic works, as well as used in political discussions, with the aim of eventually providing them with a certain degree of protection, as is the case with the ones guaranteed by international legal instruments. The first one of those to be contemplated here is the right to culture.

At a first glance, it may seem difficult to differentiate between this right and the right to take part in cultural life; nevertheless, the application of the previously outlined theoretical framework provides an explanation of the demarcation between the two. The crux of the matter, once again, lies in the difference between exclusively adopting singularism in the definition of culture, on the one hand, and recognizing both singularism and pluralism in this regard, on the other. Thus, if the notion of a "universal" culture is the only one accepted, the two

mentioned rights may be equated; yet should a distinction between a "universal" culture and the culture of a specific group be made, the two rights wind up having greatly different meanings.

The second, broader interpretation of the issue is the one adopted in this paper. Therefore, the right to culture is regarded as a strictly pluralistic projection of the otherwise mostly universalist right to take part in cultural life. The right to a culture of their own is thus bestowed upon specific groups whose binding characteristics provide a sufficient basis for the development of a particular culture. In this case, the content of the right to culture is "the respect for the cultural values of groups and individuals by others who may not share these values; [...] [that is,] the right to be different" (Stavenhagen 2001, 93).

Protection of cultural heritage – both tangible and intangible – may be considered an aspect of this right to culture. The essential objective of this protection is not the preservation of the heritage for the sake of protecting it, but rather the protection of the importance and meaning it has for the group whose culture it belongs to. This is reflected in the belief that that "for tangible and intangible cultural heritage to have meaning and potency, the heritage must be active, dynamic, used, and performed, rather than existing inert and static" (Silverman, Ruggles 2007, 12). Cultural heritage as such is often perceived as pertaining to particular cultures; nevertheless, there are certain aspects of it which may be regarded as belonging to the universal concept of culture.[1] Thus, the two conceptions of culture are connected through this right, making it contentful no matter which definition of culture is adopted.

Related to the right to culture is the concept of language rights (Pupavac 2012, 24) as well, which are sometimes considered an aspect of this broader right to culture, and sometimes considered an entirely separate cultural right. The perception of them as an aspect of the broader right to culture is derived from the understanding of languages as part of intangible culture, and thus a form of cultural heritage (Silverman, Ruggles 2007, 3). Still, they are recognized as separate rights by certain international legal instruments – the International Covenant on Civil and Political Rights (ICCPR) proclaims the right of linguistic

[1] This is often the case when it comes to cultural products created by cultures not existent anymore – e.g. the architectural achievements of Ancient Romans are nowadays perceived as belonging to the humanity as a whole, and not only to, for example, Italians as the "heirs" to the Ancient Roman culture.

minorities to use their own language (ICCPR 1966, art. 27). Accordingly, they are examined here as cultural rights on their own as well. Language rights – or, as they are often labeled, linguistic rights[2] – are founded on their relation "to the mother tongue(s) [...] consisting of the right to identify with it/them, and to education and public services through the medium of it/them" (Skutnabb-Kangas, Phillipson 1995, 71). Once again, their core is to be found in the pluralist understanding of culture, due to the fact that "language is not something enjoyed alone, but in community with others" (Pupavac 2012, 28), making it a part of the group's heritage. Thus, their protection is undeniably tied to the recognition of a group as a cultural unit, with a language specific to it, which would be offered protection through these rights.

The focal point of linguistic rights is found in the mother tongue; however, the definition of this concept may vary, which causes differing interpretations of the rights themselves. Theoretically speaking, it is possible to recognize four major approaches to the determination of a person's mother tongue – the language they first learned, the language with which they identify, the language they know the best, and the one they use the most (Skutnabb-Kangas, Phillipson 2023, 4). Depending on the criterion of definition chosen, it may happen that a person has a mother tongue they don't know (fully or at all) (Skutnabb-Kangas, Phillipson 2023, 6), which makes the protection of these rights even more complex and logistically difficult to achieve.

Seeing as linguistic rights are grounded in the group whose language they offer protection to, in practice, they are of highest importance to minority languages – when a language is spoken by a dominant group in a society, there is not as much to protect it from, making the rights less vital to enforce. The effect of the protection offered by linguistic rights is visible from the treatment the language gets – when it comes to minority languages, the approach to them is always somewhere on the "promotion continuum", going from prohibition to promotion of the language (Skutnabb-Kangas, Phillipson 1995, 79).

The relevance of the protection of linguistic rights stems from the understanding of languages as "valuable expressions of identity and culture that are linked with particular peoples" (Nic Craith 2010, 45). In

[2] Both "language rights" and "linguistic rights" are often encountered in literature, with little to no apparent difference between the two being visible most of the time. For the purposes of this paper, the two are considered coterminous, and are used interchangeably.

line with this, these rights are considered a part of identity recognition and protection (Pupavac 2012, 28), and much attention in academic works is devoted to the ways in which they are endangered, including linguicism (as analogous to racism or ethnicism) (Skutnabb-Kangas, Phillipson 1995, 105–106), linguistic imperialism (Pupavac 2012, 120–43), and even a claim that the lack of protection for linguistic rights is genocidal (Skutnabb-Kangas, Phillipson 2023, 12–13).

3. THE DIFFERENCES BETWEEN DEAF, DEAF (CAPITALIZED) AND HARD-OF-HEARING

When it comes to people whose identity in this case is defined through their different-than-ordinary situation concerning hearing, three different labels may be recognized – deaf, Deaf (with a capital letter) and hard-of-hearing. In certain cases, two labels may simultaneously be suitable for the same person, due to their differing definitions. Since the identification of a person with any one of these has specific effects on the cultural rights they have, it is necessary to clarify the distinction between the three. In order to do so, the following section focuses on two separate models of perception concerning this question.

The foundation for the differing labels lies in a set of two parallel outlooks being applied to the topic. On the one hand, the medical model recognizes two of these labels – deaf and hard-of-hearing. It is often referred to as the social model, and may be concisely defined as an audiology-based classification. On the other hand, the core of the culturo-linguistic model is removed from the medical context, and this approach is concerned with the label "Deaf".

The medical approach is grounded in the concept of deafness, "commonly understood as the partial or total absence of the faculty of hearing" (Ladd 2003, 32). The focus is placed on the biological aspect of an individual's experience – that is, the lack of functionality of the sense of hearing. The World Health Organization [WTO] recognizes four levels of hearing loss – mild, moderate, severe and profound, and these levels present the criteria for the demarcation of the deaf and hard-of-hearing labels. According to the World Health Organization (WHO), a person is considered hard-of-hearing if they have mild to severe hearing loss; if the hearing loss is profound, the person is considered deaf (WHO, 2023).

On the other hand, the culturo-linguistic approach is concerned with only one label, and that is Deafness. It has to do with much more than the level of hearing of a person, instead being connected to the experiences lived by the individual. The approach is often described along the lines of being "a Deaf counter-narrative, established [...] to counterbalance the medical and social welfare narratives which have served to 'explain' those communities to others for so many centuries" (Ladd 2003, 26), which makes it slightly more difficult to define, due to its somewhat fluid nature.

The concept of being "culturally Deaf" is sometimes described as relating to "those who grow up with 'severe' deafness as their everyday childhood reality [...] [whose] closest friends are other Deaf children, with whom they communicate in sign language [...] [who, o]n leaving school, [...] seek out local, regional, national and international groups of Deaf people, and thus become fully enculturated into Deaf communities" (Ladd 2003, 33). Such a definition provides a wide array of elements for understanding the concept; however, in practice, not all of them need be present in an individual's experience in order for them to identify as Deaf. Therein lies a certain ambiguity of the label – the absence of measurable, clear-cut criteria produces gray areas, where individuals may not obviously be part of the Deaf community, yet may show some characteristics bringing them close to the concept of Deaf culture.[3]

At its core, the concept of Deafness may be seen as a form of retaliation against being described by the hearing community as "lacking" and "less," instead identifying as simply "different." This distinction is grounded in the revolt against hearing being the standard of quality life and potential. The members of the Deaf culture often "do not view themselves as having a disability or being members of the disability community [rather perceiving] themselves as belonging to a linguistic community, full of cultural solutions" (Gertz, Boudreault 2016, 162).

As can be seen, the concept of a linguistic community is a very important one when it comes to the cultural identity of the Deaf – in effect, it may be said that "the use of and fluency in a signed language—more than the degree of sensory difference or the use of

[3] Actually, the contemporary Deaf discourse "denies that degree of hearing impairment has relevance for cultural membership" (Ladd 2003, 35); thus, a person may be medically hearing, and yet culturally Deaf – e.g. a hearing child born to Deaf parents, whose primary language is a sign language, and who was brought up in the Deaf culture.

speech as a communication technology—accounts for that defining misalignment of Deaf identity and deafness" (Harmon 2010, 34). The role of this defining element of Deafness in the understanding of the cultural rights of the members of the group is essential, especially when it comes to the cultural rights whose content depends on the pluralistic conception of culture.

When comparing the two previously outlined models, it may be pointed out that the notions of deaf and hard-of-hearing are basically defined as "hearing people who have lost some of their hearing" where "the fundamental reality is one of loss" (Ladd 2003, 33). On the other hand, the concept of Deafness is an antipode to the notion of hearing loss – it is concerned with the so-called Deaf gain, which is "a term given to the idea that the unique sensory orientation of deaf people leads to a sophisticated form of visuospatial language and visual ways of being" (Gertz, Boudreault 2016, 187). Therefore, it is the process of "reframing deafness, not as a lack, but as a form of human diversity capable of making vital contributions to the greater good of society" (Bauman, Murray 2010, 210).

In a way, being deaf may be understood in the context of

> "people who were born hearing but whose daily reality is now one of forever being condemned to live on the margins of existence, where, to adapt an old advertisement, "the edge of a conversation is the loneliest place in the world"; who have to cling to the coat-tails of the hearing world and numbly accept being reduced to imbecilic status in the eyes of the media, by cartoonists and comedians [...] [while being Deaf may be seen] as a national and international community of people with their own beautiful languages, their own organisations, history, arts and humour, their own lifelong friends whom otherwise [...] [they] would not have met" (Ladd 2003, 37).

To put it shortly, the difference between the two perspectives may be described as the difference between "the notion of audiological deafness, an audiological condition that implies no choice and no learning per se, and cultural Deafness, which implies choice and learning" (Gertz, Boudreault 2016, 286–87). When it comes to the deaf and hard-of-hearing, there is no cultural group to be recognized – therefore, the only cultural rights relevant would be the ones which regard culture as a singular, universal phenomenon. On the other hand, though, the Deaf label encompasses the concept of a cultural community, mak-

ing it suitable for the pluralistic conception of culture, and thus providing a basis for a wider array of cultural rights to be protected.

When it comes to these specific cultural rights, a claim may be encountered that "although human rights protection regimes are enacted for certain cultures, the measures do not encompass groups that are non-dominant and territorially dispersed" (Shikova, Colomina Limonero 2023, 172). While such an opinion may seem overly strong – the non-dominant and territorially dispersed groups are not absolutely deprived of the protection for their cultural rights – it does point out an issue these groups are faced with, which is a lower level of protection bestowed upon their rights.

Taking into account the peculiarities of the Deaf culture, as well as the ways in which the Deaf discourse defines this cultural group and its core elements, it may be concluded that linguistic rights are the most important ones to be protected when it comes to this group. However, the obstacles for this are manifold. Apart from the already mentioned territorial dispersion and non-dominant status of the group in question (the Deaf community), an issue also arises from the lack of understanding that sign languages are languages in their own right.

Sign languages are often seen as purely interpretative mechanisms applied to the existing, spoken languages, despite it not being true. While their protection is enshrined in the Convention on the Rights of Persons with Disabilities (CRPD 2007) – through the recognition of the specific cultural and linguistic identity of persons with disabilities (art. 30.4), recognizing and promoting the use of sign languages (art. 21.1), and facilitating the learning of sign language and the promotion of the linguistic identity of the deaf [*sic*] community (art. 24.3) – in practice, this is not done to a satisfactory degree. Taken altogether, the aforementioned factors make the protection of cultural rights of the Deaf much more difficult and less effective.

4. DIGITAL TECHNOLOGIES AFFECTING THE CULTURAL RIGHTS OF D/DEAF AND HARD-OF-HEARING PEOPLE

The impact of digital technologies and their expansion can be felt in a vast number of areas of life of a person, be they d/Deaf or hard-of-hearing, or not. Such is the case with the cultural rights of d/Deaf and hard-of-hearing persons as well, which is the focus of this

paper. In order to best address the issue at hand, the following section shall first address the types of different digital technologies relevant to the topic, and then provide an analysis of their impact on the cultural rights of d/Deaf and hard-of-hearing people.

4.1. Types of Relevant Digital Technologies

The variety of digital technologies relevant for this topic is considerable; however, only the most impactful and widespread ones are examined in the following section. Among the referenced technologies, two broader categories may be recognized – assistive technologies, and ordinary-use technologies which still impact the cultural rights of the d/Deaf and hard-of-hearing people. Their analysis is approached accordingly, with attention first being given to one, and then the other category.

Assistive technologies are created with the purpose of helping a person overcome the limitations placed upon them due to a form of reduced ability, or disability, they have. These technologies can be developed in the form of physical products (when it comes to the d/Deaf and hard-of-hearing, an example for these would be hearing aids or cochlear implants) or digital products (e.g. software and apps that support interpersonal communication) (WHO, 2022). Obviously, the physical products have a longer history of usage; nevertheless, the corpus of digital products available for these purposes is rapidly growing, making it equally suitable for analysis. At the same time, it is necessary to point out that, despite their division into physical and digital ones, all the products discussed here rely on digital technologies in order to function, at least in their contemporary versions.

The oldest form of assistive technologies for the d/Deaf and hard-of-hearing are hearing aids (Valentinuzzi 2020). Their structure and functions have evolved through the time; nevertheless, substantially they remain devices which are inserted into the ear in a non-invasive way, with the aim of helping a person who has a certain level of hearing left gain more information from the existing sound stimuli from their environment. Contemporary hearing aids – as opposed to those from the predigital era, when they were little more than amplifiers – combine amplification with "advanced forms of signal processing for speech enhancement, noise reduction, self-adapting directional inputs, feedback cancellation, data monitoring, and acoustic scene analysis, as

well as the means for a wireless link with other communication systems" (Levitt 2007, 7). Thus, they provide the user with significant help in processing sounds around them.

Another form of a physical product devised as an assistive technology for the d/Deaf and hard-of-hearing are cochlear implants. Similarly to hearing aids, cochlear implants are also equipped with digital technology – still, in order to use them, a person must undergo a surgical intervention which places a part of the device inside the skull, making this a much more invasive form of assistive technology. Due to the serious nature of the procedure, their use is reserved for those with profound hearing loss – that is, for cases in which hearing aids are incapable of causing improvement. At the same time, even though cochlear implants can be used in cases of adult deafness, most cases – and most attention in the narratives concerning this type of assistive technology – are of children, especially very young ones, receiving this kind of treatment.

When it comes to the digital products of assistive technologies, a greater variety may be recognized. Their proliferation and development is constant and rapid, providing a huge body of possible objects of analysis; nevertheless, attention will be devoted to three main categories of such technologies – closed captioning, speech recognition and live captioning, and sign language generation and interpretation software.

Closed captioning is mainly understood as pertaining to pre-existent content, and it is used as a means of making its audio elements accessible to d/Deaf and hard-of-hearing people. Although similar to the process of subtitling, this process requires special training (as compared to the interlingual subtitling for the hearing) (Neves 2008, 135), since there is an additional need for "descriptions of sound effects, background noises and other vital information which may be required for Deaf [...] [people] to fully comprehend the content of the [...] materials" (Ohene-Djan, Shipsey 2006, 1). In comparison, subtitling is a process which consists of translating the content from one language to another, and it conveys only the spoken information (United Nations 2022, 41), omitting other audio content. An overlap between the two may be recognized in subtitles for the d/Deaf and hard-of hearing – these are used when content is translated (which is the subtitling aspect of the process), as well as enriched through the inclusion of other, non-spoken audio content in its creation (the closed captioning aspect of the process) (United Nations 2022, 41).

When it comes to closed captioning, the aim is to make as much audio content accessible to the viewer as can be done. However, it is very difficult (if not absolutely impossible) to convey the full message originally transmitted orally, through a written medium. The words may be transcribed; yet the intonation, speed of speech, emotions etc. cannot be fully translated to the written word. There have been some ideas for including the emotional aspect of the words spoken by characters through the usage of different colors, fonts etc. (Ohene-Djan, Shipsey 2006), still, even if this were to be included in all cases, a risk of overcrowding the script would be present, reducing its reliability and usefulness.

The danger of overcrowding the script is even more of an issue when its users are Deaf. In this case, their mother tongue is a sign language – therefore, the script is given in a language that is second to them, which makes it more difficult to follow (Neves 2008, 131). At the same time, generally speaking, the Deaf often read slower – research suggests that they may find information "more accessible when it is provided in a video format with sign language, rather than in a text format" (United Nations 2022, 23). Obviously, this makes subtitles more difficult to follow as well (Neves 2009, 159–60).

A lack of these technologies lies in their primary use for premade content; that is, their lack of applicability in real-time situations. In order to provide accessibility to d/Deaf and hard-of-hearing people in these contexts as well, other technologies are used, such as speech recognition systems and live captioning. Automated systems may be used to this effect, but it is not the only option – live captioners may be human too; however, professionals in this field are rare, and their services are quite expensive, making this approach less accessible (Kawas et al. 2016, 1).

When it comes to using automatic speech recognition software for communication between hearing and d/Deaf or hard-of-hearing people, research suggests that it is a system faster than typing messages (Stinson et al. 2017). Such a claim may be understood as justification for the development of some software in this area – for example, a French company created an application which uses speech-to-text algorithms in order to make phone calls accessible to d/Deaf and hard-of-hearing people. Apparently, systems like these can have an up to

93% accuracy result, with the possibility of it getting higher with the slowing down of dictation (Lyall, Clamp, Hajioff 2016, 106); still, this is not always true, and "errors in live-captioning tools, while they might seem acceptable to hearing individuals, can exclude deaf users depending on it to follow a conversation" (Touzet 2023, 29).

A more elaborate idea, whose foundation is in these technologies, is the development of an augmented reality in conjunction with an automatic speech recognition (or audio-visual speech recognition) system to help in communication, by making "speech bubbles" appear next to the speaker on a video stream, so that the user experiences communication in a way similar to a comic book (Mirzaei, Ghorshi, Mortazavi 2012). The potential of such a solution is undeniable; yet it must be emphasized that such ideas are only in their development stages, and much more work has to be done in order of them to be reliable enough to be widely used.

Finally, there has been mention of ways to develop sign language generation and interpretation software in the interface of computing systems, with the aim of making access to them easier (Huenerfauth, Hanson 2009). The idea for the creation of such tools has great merit; nevertheless, its development can be rather demanding, both in terms of financial resources and time needed to be devoted to the process. At the same time, relevant stakeholders may not always be motivated enough to invest in such endeavors. Consequentially, the level of development of these technologies is quite low, and the attention devoted to the improvement of this situation quite little.

In the end, technologies which are not assistive in nature, yet have some impact on the cultural rights of the d/Deaf and hard-of-hearing people, should be mentioned. Ordinary subtitling may be considered a part of this category – though it is not as effective as some of the assistive technologies discussed above, in the absence of anything better, a subtitle can provide some help to d/Deaf and hard-of-hearing people when it comes to accessing audio content. Incidental benefits for these individuals may come from video conferencing software as well – although sign communication taking place in digital space is different from the "live" version (Keating, Edwards, Mirus 2008), it still makes communication from afar possible, which is an improvement compared to the times where live communication could only be achieved in audio form.

4.2. The Effect of the Examined Digital Technologies on the Cultural Rights of d/Deaf and Hard-of-Hearing People

When it comes to the cultural rights of d/Deaf and hard-of hearing people, the effects these technologies have on them are quite diverse. Some cultural rights seem to mostly benefit from the majority of technologies shown; on the other hand, in certain cases, the situation is much less clear. The following section provides an overview of the effects recognized in the fields of all previously defined cultural rights of d/Deaf and hard-of-hearing people.

The results of introducing the examined digital technologies into the lives of d/Deaf and hard-of-hearing people in regards to the status of their cultural rights are most controversial in the cases of the right to culture and the protection of cultural heritage. As is guaranteed by the CESCR, everyone has "the right to choose one's own identity, identify or not with one or more communities, or to change that choice" (CESCR 2009, para. 15a). Consequently, the Deaf community, as the proprietary of Deaf culture and, thus, the subject of the right to culture tied to it, often raises the argument of a number of these technologies being an attempt to force hearing culture upon them, and thus suppress their own cultural identity.

This is especially visible when it comes to the physical assistive technologies discussed above (hearing aids and cochlear implant. In fact, "[w]hile some, especially post-lingually deaf people may embrace the technology, those who see themselves as a cultural or linguistic minority and refuse to see their worlds as tragically silent have reauthored biomedical narratives in a way that depicts a colonial force" (Roulstone 2016, 23–24). Due to their invasiveness, cochlear implants tend to be even more susceptible to such aversion than hearing aids are (Sparrow 2010).

The distinction, as can be seen, stems from the difference between deaf/hard-of-hearing and Deaf people. It may be said that "those coming from a medical standpoint [...] see cochlear implants as a "cure" for deafness, and those who came from a Deaf perspective [...] view cochlear implants as a violation of [...] [a person's] right to be Deaf" (Archbold, Wheeler 2010, 227). Therefore, when it comes to the protection of the cultural rights of deaf and hard-of-hearing people, these technologies are often seen as beneficial – they may make it easier for their users to access culture, get an education etc. However,

when regarded from the perspective of protecting the cultural rights of the Deaf, they are considered a threat to their particular cultural rights.

The complaints shown above are most often raised by Deaf parents of a child who is a potential user of such technologies. A question may be raised, though, if the usage of these technologies can really endanger an individual's right to culture – that is, their right to be Deaf. As has been mentioned before, the cultural concept of Deafness is not necessarily tied to the medical notion of deafness; therefore, it may be pointed out that

> "The majority of models and discussion of the makeup of the Deaf community seem to accept the inevitability that hearing people will be members of the community—up to a point. The focus in this context is often on those hearing people that have Deaf parents or siblings and have therefore grown up in the Deaf community, acquired sign language from an early age, and become enculturated to the Deaf way of life" (Napier 2002, 142).

Therefore, a child can be Deaf even if, through the use of technologies such as these, they are not deaf or hard-of-hearing. In this case, the impact of technologies is such that it only gives the child the possibility to "benefit from the cultural heritage and the creation of other individuals and communities", which is determined to be part of the right to take part in cultural life (CESCR 2009, para. 15b).

The technologies discussed here could be perceived as endangering the right to protection of cultural heritage. It may be said that this and the right to culture are very closely tied – however, while the right to culture may be understood as an individual, as well as a communal right, the protection of cultural heritage is fundamentally focused on the social unit as its subject. Through the application of technologies which provide persons who would otherwise be exclusively Deaf when it comes to the cultural divide between Deaf and hearing worlds with means to become a part of the hearing culture as well, the incentive for participation in Deaf culture for these individuals grows weaker. With the passage of time, this can bring about a considerable reduction in the size of the Deaf community (Sparrow 2010, 3–4), thus endangering the Deaf culture as a part of cultural heritage.

An argument could be raised that, in individual cases, the benefits a person (in most cases concerning e.g. cochlear implants, a child) receives from the application of relevant digital technologies should

take primate over the interests of the communal good of cultural heritage. Such a claim could be defended through the principle of acting "in the best interests of the child", which is enshrined in the Convention on the Rights of the Child (1989, art. 3.1). Still, such arguments often ride the fine line between true protection of human rights, and outright cultural imperialism. Therefore, it comes as no surprise that the debate between the two cannot be clearly resolved.

Arguments similar to those concerning physical assistive technologies may be applied to a number of other technologies considered in this paper. Closed captioning, speech recognition softwares, live captioning and ordinary subtitling all have the same issue of forcing hearing culture upon a d/Deaf or hard-of-hearing person, instead of providing a way for the relevant content to be transposed into a form compatible with their own cultural experiences. On the other hand, this issue is avoided in cases of sign language generation and interpretation software, as well as video conferencing systems – these are considered truly beneficial for the right to culture of the d/Deaf and hard-of-hearing people.

Closely related to the topics of the right to culture and the protection of cultural heritage is the issue of linguistic rights, so it comes as no surprise that the arguments pertaining to these questions have a great deal of overlap. The same set of technologies seen as negative when it comes to the right to culture and the protection of cultural heritage, is considered to have a negative effect on the linguistic rights, due to them negatively impacting the incentive for learning sign languages, which are considered mother tongues of Deaf individuals. On the other hand, the technologies whose objective is not replacing sign languages, but rather providing them with a means of more efficient transmission and application – such as sign language generation and interpretation software, as well as video conferencing systems – are considered beneficial to the state of protection of these rights.

The impact of discussed digital technologies is visible in the area of the right to take part in cultural life as well. In this regard, the effects are mostly positive, and can be observed both when it comes to the question of media content, where closed captioning and ordinary subtitling provide a way for d/Deaf and hard-of-hearing individuals to access it, and in the field of live communication, where technologies such as speech recognition software and live captioning act as a tool for communicating with hearing individuals. Improvement is noted in

both these contexts when it comes to hearing aids and cochlear implants as well, while sign language generation and interpretation software, as well as video conferencing systems, have a somewhat limited scope of impact when it comes to the participation of d/Deaf and hard-of-hearing individuals in the universal cultural life, seeing as their function is primarily confined to the inside of the Deaf community.

Concerning the right to education, it may be said that many of the mentioned technologies have the potential of improving the accessibility of education in general. This is true for the physical products of assistive technologies – hearing aids and cochlear implants – but also for other tools. Closed captioning and ordinary subtitling provide d/Deaf and hard-of-hearing students with a way to use otherwise inaccessible teaching materials, such as audio recordings, videos with relevant sound content, and the likes. On the other hand, speech recognition software and live captioning facilitate communication with hearing instructors, as well as make it possible for d/Deaf and hard-of-hearing students to participate in interactive work during classes, along with their hearing peers.

However, it must be emphasized that the right to education is not confined to its aspect of accessibility. Rather, when it comes to the topic at hand, it is necessary to mention the elements of acceptability of education (which means, *inter alia*, that it is culturally appropriate to students), as well as its adaptability (*inter alia,* to the "needs of changing societies and communities [...] and the needs of students within their diverse social and cultural settings" (CESCR 1999, para. 6). Taking these into account, it may be claimed that shortcomings are recognizable in all the technologies previously criticized for infringing on the right to culture, protection of cultural heritage and/or linguistic rights of d/Deaf and hard-of-hearing people.

Finally, when it comes to the right to enjoy the benefits of scientific progress and its applications, as has been mentioned in the theoretical framework of the paper, the two most relevant aspects to be considered are the right to access to results of scientific progress, and the right to participation in decision-making concerning it. Evidently, the rise of the number and diversity of digital technologies which can be used by d/Deaf and hard-of-hearing can be taken for a positive effect on the right to access to scientific progress. On the other hand, when it comes to the right to participation in the decision-making process concerning scientific progress, the basis for its protection can be

found in the soft law of the Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities, in the provision saying that "[p]ersons belonging to minorities have the right to participate effectively in decisions on the national and, where appropriate, regional level concerning the minority to which they belong or the regions in which they live, in a manner not incompatible with national legislation" (1992, art. 2.3). Basically, in order for more useful and accessible technology to be made, its potential users must have a say in the process, providing the needed guidance for and pressure on the relevant stakeholders. An elaboration of this is provided in the following section.

5. STRATEGIES FOR IMPROVEMENT

As has been shown in the previous part of the paper, the effect digital technologies have on the cultural rights of the d/Deaf and hard-of-hearing people are varied – there is much potential for them to be beneficial, yet they also produce a number of negative side effects. Moving forward, in order to maximize the benefits which digital technologies may provide in this regard, while neutralizing as many of their negative effects as possible, it is necessary to introduce some changes. Different approaches should be applied to different actors in the system; therefore, a specialized strategy must be devised for the Deaf community, the broader hearing community, the relevant stakeholders and the state actors.

When it comes to the Deaf community, it is necessary to give them more power in the process of decision-making concerning digital technologies developed for their needs. They must be given a voice to advocate for their own cultural interests, thus ensuring those are not overlooked for the sake of the interests of other involved actors. At the same time, when faced with unsuitable or insufficiently effective technological solutions, they must be encouraged to point out the shortcomings of the tools they are offered, so that the illusion of their absolute sufficiency can be dismantled.

When it comes to the broader hearing community, effort must be directed towards educating its members on the challenges d/Deaf and hard-of-hearing people face, as well as on the cultural particularities of the Deaf community. While some hearing people may be aware

of those, yet unwilling to act in accordance with the best interests of the d/Deaf and hard-of-hearing people, a significant portion of the hearing community simply does not know enough about the situation at hand. The importance of this lies not only in the way these hearing individuals will treat the d/Deaf and hard-of-hearing people they interact with, but also in the assistance they may give in exacting pressure on the relevant stakeholders when it comes to the protection of the interests of d/Deaf and hard-of-hearing people.

Education and informing efforts may prove to be helpful when it comes to the relevant stakeholders themselves as well. Presenting the benefits which could be achieved through the development of truly effective digital technologies, as well as a just application of those, may motivate the stakeholders to invest their resources and political power in making such goals a reality. Even though the effects might not be apparent in all cases, differences between the stakeholders may also prove to be beneficial – those who recognize the importance of this topic will gain an advantage in developing relevant technologies, thus becoming more competitive on the market. At the same time, their reputation will benefit from the status of being open to the interests of minority groups such as the d/Deaf and hard-of-hearing communities, providing them with further advantage in the eyes of their customers.

Finally, when it comes to the state actors, they need to be proactive in providing suitable protection to the cultural rights of the Deaf. This should be done through preemptive measures of preservation of the Deaf culture, in order to prevent its dying off due to a perceived "lack of need for it". Achieving this can be done in part through legislation; however, the engagement of state actors should go further than that, extending into the areas of public policy and general political involvement.

6. CONCLUSION

The presence of digital technologies is becoming all the more encompassing as time goes, and their effects are getting all the more pronounced in all areas of people's lives. The same holds true for the effects they have on the cultural rights of d/Deaf and hard-of-hearing people. Due to the wide scope of their interference in the daily lives of their users, as well as the diversity of their forms and objectives, it

comes as no surprise that the consequences of their usage can be both positive and negative, depending on the case.

The benefits provided by these technologies are highly visible in their impact on the right to education. The correct application of suitable digital technologies in this sense provides a way for d/Deaf and hard-of-hearing people to understand instruction, as well as gain access to various teaching materials. Similar effects may be recognized in the case of the right to take part in cultural life – through the application of these technologies, otherwise inaccessible cultural content is made suitable for these individuals to consume. Nevertheless, the situation is not without drawbacks.

First of all, the ways in which the majority of the examined digital technologies tackle the issues faced by the d/Deaf and hard-of-hearing people, focus on getting these individuals to participate in the hearing world, without taking into account their own cultural solutions to the challenges they face. Lack of ability to participate in the hearing world unaided is regarded as a shortcoming, and the digital technologies are seen as a tool for "fixing" this. Such an attitude overlooks the value Deaf culture has, and reduces it to an inferior way of life, one the members of this group presumably lead only out of a lack of choice, which is contradictory to the perception of Deaf culture its members actually have.

Another issue with the technological solutions discussed in this paper is their lack of satisfactory results. As has been pointed out, none of these technologies provide ideal results – however, hearing people may often be unaware of this fact. Therefore, seeing that the technologies mentioned are aiding d/Deaf and hard-of-hearing people, they may conclude there to be no need for further aid and support, even though the help provided by the technologies is not enough to put the d/Deaf and hard-of-hearing at an equal level of accessibility as the hearing people in the same situation. Consequently, even if the goal of the d/Deaf and hard-of-hearing people were to simply become integrated in the hearing world, disregarding their own cultural particularities, this would not be enough for such a result to be achieved.

Finally, the danger these technologies may pose to the Deaf culture as a communal good cannot be overlooked. Some of them are outwardly considered an affront to their cultural rights by the Deaf community – such as cochlear implants. On the other hand, even those technologies which the community regards as beneficial to them, may

prove to be detrimental to their cultural rights in the long run. Once again, the reason for this lies in the perception of the hearing people – seeing the ways in which these technologies increase accessibility for d/Deaf and hard-of-hearing people, they may come to the conclusion that Deaf culture and language "no longer necessary". Obviously, this would bring about a reduction in the protection offered to these cultural rights.

In the end, it may be concluded that, while digital technologies may be beneficial to the state of the cultural rights of d/Deaf and hard-of-hearing people, they may also be detrimental in certain cases. That is not to say that the technologies themselves are either good or bad; on the contrary, the responsibility for making sure their positive effects are maximized, and their negative effects made as small as possible, lies with those making decisions on how the technologies are used, and how the general public is informed about the results they can(not) provide. Future actions regarding this question have the power to minimize the recognized negative effects, while preserving and ameliorating the possible benefits; however, in order for this to be done, a number of diverse, relevant actors must put in a significant amount of effort. Whether this will happen in the proximate future or not, remains to be seen.

REFERENCE LIST

1. Archbold, Sue, Alexandra Wheeler. 2010. Cochlear Implants: Family and Young People's Perspectives. 226–40 in *The Oxford Handbook of Deaf Studies, Language, and Education*, edited by Marc Marschark and Patricia Elizabeth Spencer. Oxford Library of Psychology. Oxford: Oxford University Press.
2. Bauman, H.-Dirksen L., Joseph J. Murray. 2010. Deaf Studies in the 21st Century: 'Deaf-Gain' and the Future of Human Diversity. 210–35 in *The Oxford Handbook of Deaf Studies, Language, and Education*, edited by Marc Marschark and Patricia Elizabeth Spencer. Oxford Library of Psychology. Oxford: Oxford University Press.
3. Chow, Pok Yin Stephenson. 2014. Culture as Collective Memories: An Emerging Concept in International Law and Discourse on Cultural Rights. *Human Rights Law Review* 14 (4): 611–46.
4. Gertz, Genie, Patrick Boudreault, eds. 2016. *The Sage Deaf Studies Encyclopedia*. Los Angeles: SAGE reference.

5. Harmon, Kristen. 2010. Deaf Matters: Compulsory Hearing and Ability Trouble. 31–47 in *Deaf and Disability Studies: Interdisciplinary Perspectives*, edited by Susan Burch and Alison Kafer. Washington, DC: Gallaudet University Press.
6. Huenerfauth, Matt, Vicki L. Hanson. 2009. Sign Language in the Interface: Access for Deaf Signers. 1–18 in *The Universal Access Handbook*, edited by Constantine Stephanidis. Human Factors and Ergonomics. Boca Raton: CRC Press.
7. Kawas, Saba, George Karalis, Tzu Wen, Richard E. Ladner. 2016. Improving Real-Time Captioning Experiences for Deaf and Hard of Hearing Students. 15–23 in *Proceedings of the 18th International ACM SIGACCESS Conference on Computers and Accessibility*. Reno Nevada USA: ACM.
8. Keating, Elizabeth, Terra Edwards, Gene Mirus. 2008. Cybersign and New Proximities: Impacts of New Communication Technologies on Space and Language. *Journal of Pragmatics* 40 (6): 1067–81.
9. Ladd, Paddy. 2003. *Understanding Deaf Culture: In Search of Deafhood*. Clevedon, England; Buffalo: Multilingual Matters.
10. Levitt, Harry. 2007. A Historical Perspective on Digital Hearing Aids: How Digital Technology Has Changed Modern Hearing Aids. *Trends in Amplification* 11 (1): 7–24.
11. Lyall, Fiona, Philip Clamp, Daniel Hajioff. 2016. Smartphone Speech-to-Text Applications for Communication with Profoundly Deaf Patients. *The Journal of Laryngology & Otology* 130 (1): 104–6.
12. Mirzaei, Mohammad Reza, Seyed Ghorshi, Mohammad Mortazavi. 2012. Using Augmented Reality and Automatic Speech Recognition Techniques to Help Deaf and Hard of Hearing People. *Laval Virtual VRIC '12*.
13. Napier, Jemina. 2002. The D/Deaf – H/Hearing Debate. *Sign Language Studies* 2 (2): 141–49.
14. Neves, Josélia. 2008. 10 Fallacies about Subtitling for the d/Deaf and the Hard of Hearing. *The Journal of Specialized Translation*, no. 10: 128–43.
15. Neves, Josélia. 2009. Interlingual Subtitling for the Deaf and Hard-of-Hearing. 151–69 in *Audiovisual Translation: Language Transfer on Screen*, edited by Jorge Díaz-Cintas and Gunilla M. Anderman. Basingstoke [England] ; New York: Palgrave Macmillan.
16. Nic Craith, Máiréad. 2010. Linguistic Heritage and Language Rights in Europe: Theoretical Considerations and Practical Implications. 45–62 in *Cultural Diversity, Heritage and Human Rights: Intersections in Theory and Practice*, edited by Michele Langfield, William Stewart Logan, and Máiréad Nic Craith. Key Issues in Cultural Heritage. London; New York: Routledge.

17. Ohene-Djan, James, Rachel Shipsey. 2006. E-Subtitles: Emotional Subtitles as a Technology to Assist the Deaf and Hearing-Impaired When Learning from Television and Film.1–3 in *Proceedings of the Sixth International Conference on Advanced Learning Technologies*. Kerkrade, The Netherlands.
18. Pupavac, Vanessa. 2012. *Language Rights: From Free Speech to Linguistic Governance*. Palgrave Studies in Minority Languages and Communities. Basingstoke; New York: Palgrave Macmillan.
19. Roulstone, Alan. 2016. *Disability and Technology: An Interdisciplinary and International Approach*. London: Palgrave Macmillan.
20. Shikova, Natalija, Immaculada Colomina Limonero. 2023. Can Non-Territorial Autonomy Help to Enforce the Linguistic, Cultural and Educational Rights of the Roma. 171–94 in *Realising Linguistic, Cultural and Educational Rights Through Non-Territorial Autonomy*, edited by David J. Smith, Ivan Dodovski, and Flavia Ghencea. Cham: Springer Nature Switzerland.
21. Silverman, Helaine, D. Fairchild Ruggles. 2007. Cultural Heritage and Human Rights. 3–22 in *Cultural Heritage and Human Rights*, edited by Helaine Silverman and D. Fairchild Ruggles. New York, NY: Springer.
22. Skutnabb-Kangas, Tove, Robert Phillipson. 1995. Linguistic Human Rights, Past and Present. 71–110 in *Linguistic Human Rights: Overcoming Linguistic Discrimination*, edited by Tove Skutnabb-Kangas and Robert Phillipson. Berlin New York: Mouton de Gruyter.
23. Skutnabb-Kangas, Tove, Robert Phillipson. 2023. Introduction: Establishing Linguistic Human Rights. 1–22 in *Handbook of Linguistic Human Rights*, edited by Tove Skutnabb-Kangas and Robert Phillipson. Blackwell Handbooks in Linguistics. Hoboken, NJ: Wiley.
24. Smith, Rachel Craufurd. 2007. The UNESCO Convention on the Protection and Promotion of Cultural Expressions: Building a New World Information and Communication Order?. *International Journal of Communication* 1: 24–55.
25. Sparrow, Robert. 2010. Implants and Ethnocide: Learning from the Cochlear Implant Controversy. *Disability & Society* 25 (4): 455–66.
26. Ssenyonjo, Manisuli. 2016. *Economic, Social and Cultural Rights in International Law*. Oxford; Portland, Oregon: Hart Publishing.
27. Stavenhagen, Rodolfo. 2001. Cultural Rights: A Social Science Perspective. 85–110 in *Economic, Social, and Cultural Rights: A Textbook*, edited by Asbjørn Eide, Catarina Krause, and Allan Rosas. Dordrecht; Boston; London: Martinus Nijhoff Publishers.
28. Stinson, Michael, Syed Ahmed, Lisa Elliot, and Donna Easton. 2017. Using Automatic Speech Recognition to Facilitate Communication Between an Individual Who Is Hearing and One Who Is Deaf or Hard of Hearing.

407–8 in *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility*. Baltimore Maryland USA: ACM.

29. Stojković, Branimir. 1999. Identitet kao determinanta kulturnih prava. 9–97 in *Kulturna prava*, edited by Vojin Dimitrijević, Agneš Kartag-Odri, Branislav Milinković, Jan-Lui Serfontein, Ivana Simović-Hiber and Branimir Stojković. Beograd: Beogradski centar za ljudska prava.
30. Touzet, Chloe. 2023. Using AI to Support People with Disability in the Labour Market. *OECD Artificial Intelligence Papers*, no. 7.
31. UN General Assembly. 1948. Universal Declaration of Human Rights. *https://www.refworld.org/docid/3ae6b3712c.html* (last visited 31 January, 2024).
32. UN General Assembly. 1966. International Covenant on Economic, Social and Cultural Rights. *https://www.refworld.org/docid/3ae6b36c0.html* (last visited 31 January, 2024).
33. UN General Assembly. 1966. International Covenant on Civil and Political Rights, *https://www.refworld.org/docid/3ae6b3aa0.html.* (last visited 31 January, 2024).
34. UN General Assembly. 1989. Convention on the Rights of the Child. *https://www.refworld.org/docid/3ae6b38f0.html.* (last visited 31 January, 2024).
35. UN General Assembly. 2007. Convention on the Rights of Persons with Disabilities. *https://www.refworld.org/docid/45f973632.html.* (last visited 31 January, 2024).
36. UN General Assembly. 1992. Declaration on the Rights of Persons Belonging to National or Ethnic, Religious and Linguistic Minorities. *https://www.ohchr.org/en/instruments-mechanisms/instruments/declaration-rights-persons-belonging-national-or-ethnic.* (last visited 31 January, 2024).
37. UN Committee on Economic, Social and Cultural Rights. 1999. General Comment No. 13: The Right to Education (Art. 13 of the Covenant). *https://www.refworld.org/docid/4538838c22.html* (last visited 31 January, 2024).
38. UN Committee on Economic, Social and Cultural Rights. 2009. General Comment No. 21, Right of Everyone to Take Part in Cultural Life (Art. 15, Para. 1a of the Covenant on Economic, Social and Cultural Rights). *https://www.refworld.org/docid/4ed35bae2.html* (last visited 31 January, 2024).
39. Valentinuzzi, Max E. 2020. Hearing Aid History: From Ear Trumpets to Digital Technology. *IEEE Pulse* 11 (5): 33–36.
40. Veriava, Faranaaz, Kate Paterson. 2020. The Right to Education. 113–36 in *Research Handbook on Economic, Social and Cultural Rights as Human Rights*, edited by Jackie Dugard, Bruce Porter, Daniela Ikawa and Lilian Chenwi. Cheltenham, UK ; Northampton, MA, USA: Edward Elgar Publishing.

41. Woods, Jeanne M. 2005. Emerging Paradigms of Protection for 'Second-Generation' Human Rights. *Loyola Journal of Public Interest Law* 6: 103–28.
42. World Health Organization. 2022. Global Report on Assistive Technology. *https://iris.who.int/bitstream/handle/10665/354357/9789240049451-eng.pdf?sequence=1* (last visited 31 January, 2024).
43. World Health Organization. 2023. Deafness and Hearing Loss Factsheet. *https://www.who.int/news-room/fact-sheets/detail/deafness-and-hearing-loss* (last visited 31 January, 2024).

UDK 347.775:004.738.5
DOI 10.51204/IVRS_24104A

Dušan Samardžić*

A DELEUZIAN PERSPECTIVE ON THE RIGHT OF DATA PROTECTION ON SOCIAL MEDIA

The goal of this article is to explore – from the given theoretical framework – the effectiveness of the European Union's data protection capabilities, namely through the General Data Protection Regulation. The first and second sections develop the theory of control societies – as well as its historical background – and connects it with the theory of surveillance capitalism as its essential component. The third section delas with some critiques that have arisen in the few years after the GDPR came into force. The conclusion of the paper is that, only a few years after the GDPR came into force, it is still too early to decisively say what effect will it have on the big data industry. However, from the problems that have been elaborated, it seems unlikely that the big data industry will be meaningfully challenged when it comes to data protection.

Key words: *control societies, big data, Surveillance capitalism, general data protection regulation, data analysis.*

1. INTRODUCTION

Over the course of the last few decades there has been a unique trend of personal data exploitation that came to be wide spread with the massive expansion of digital technology especially with those that facilitate a large amount of data sharing. Concerns have been raised about the ways how this can infringe on fundamental rights, such as the right to privacy and data protection, as guaranteed by relevant domestic and international sources of law. To do so, one must adopt an analytic framework for understanding the phenomena at hand. As the title suggests, this will be attempted with the help of the post-structuralist theory of Gilles Deleuze as well as others.

* The author is a fourth-year undergraduate student at the University of Belgrade Faculty of Law, *samardzicd01@gmail.com*.

The paper is broadly separated into three subsections. The first subsection of the paper is concerned with explaining the theoretical background as conceived by Michel Foucault which Deleuze used as foundation for further development of his own theory. Through the analysis of the tools of sovereign and disciplinary societies, the ways in which control societies differ from them is portrayed, as well as which elements of sovereign and discipline societies still exist in the modern day. The second section deals with the very notion of control societies. Important concepts such as the dividual are defined so that this broad theory pointing at new ways modern technology and a change in subjectivity can be used for control can be set for concretization of the problem at hand. This is then done through the analysis of Shoshana Zuboff's concept of surveillance capitalism and its ways data is commodified. After explaining the ways this new form of commodification is performed, a part is dedicated to contextualizing the concept of surveillance capitalism within the Deleuze's theory of control societies. Finally, the third section is concerned with exploring the ways data is protected under the General Data Protection Regulation (GDPR) and critiques that may arise from the viewpoint of the presented theories.

At the end, the results of research are contemplated and a conclusion will be given that primarily tries to give a diagnose and explore some of the possible outcomes for the future of data protection after considering various problems that can arise during the enforcement of the GDPR.

2. HISTORICAL BACKGROUND

As Deleuze's analysis of modern societies is contingent upon the historical framework of his contemporary Foucault, we must first portray a sort of genealogy of power and the way it was exercised over legal subjects throughout history according to Foucault's theory.

2.1. Societies of sovereignty

Foucault defined power in relation to its object of control. In the case of what he identified as the ancient form of power, that would be the power over life and death. The first mention of sovereign power as the right over life and death came in *The History of Sexuality, Vol.*

1, in contrast to the notion of bio-power. Sovereign power, he claims, had its roots in ancient Rome in the form of the father's *patria potestas,* which over time transformed into an indirect right of the sovereign of retaliation (Foucault 1976, 135). Therefore, the right of the sovereign was manifested directly only in the case of transgression against him, and up until then it was only hypothetical.

Foucault claims (1976, 135–136) that this perspective is contrasted to the classical view of social contract theories epitomized in Thomas Hobbes since he does not claim that the power of the sovereign comes from the yielding of sovereignty innate in humans, but rather as a new right that came with the creation of "a new juridical being, the sovereign". Here we see Foucault's shift from dialectical explanations of history, explaining change as a result of societal struggle, to a non-systematic Nietzschean genealogy of change (Nietzsche 1990).

Compared to modern societies, sovereign societies functioned on the principle of "deduction"-namely, the right to take something away. Primarily, this meant that the ruler had the right to take a portion of his subjects' wealth, and even their life by asking them to wage war for him as mentioned before – this being most visible through the death penalty as a result of disobedience (Guttig, Oskala 2022)[1]. The principle of deduction also manifested itself in the form of exclusion and exile. Sovereign power is not totalitarian, it does not "...combine and compose, [it is used] to divide the masses rather than to isolate the detail; to exile rather than to seal off (its model is that of 'leprosy')" (Deleuze 1988, 35).

In short, sovereign societies were in a sense characterized by freedom so long as the subject refrained from threatening the sovereign – his legal order. Other than that, much of his life was left up to him to decide – a characteristic that stands in stark contrast to disciplinary societies.

2.2. Disciplinary societies

With the emergence of disciplinary societies in the 18th and 19th centuries, culminating in the 20th century, the object of power changed. The goal of power was no longer to tax but to organize production; not to rule on death, but to administer life (Deleuze 1997, 177–178). This means that the sovereign was only concerned with deducing, that

[1] See also: Stanford Encyclopedia of Philosophy, 2022a.

is, taking away what was his under the law– a portion of the serf's produce, for example – but he wouldn't go so far as to determine the serf's work schedule, shape his production, etc. In disciplinary societies, however, with the emergence of capitalism and industrialization, work became organized in a way to, among other goals, maximize production efficiency. The right of death, in a similar way, became secondary to the administration of life. What Deleuze referenced here was Foucault's concept of biopower. Unlike the right over life and death, biopower is positive, it seeks to "... exert a positive influence on life, that endeavors to administer, optimize, and multiply it, subjecting it to precise controls and comprehensive regulations" (Foucault 1976, 137). This, however, does not mean that the right over life and death is replaced with this softer power, but rather that it co-exists in the negative – in Foucault's formula "kill or let live" (Protevi 2009, 59), which is now reserved for only the most egregious of crimes – but also transforming into other indirect forms. Institutes like general conscription only came into existence with the advent of the French Revolution and became a symbol of biopower. Bodies are instructed and formed in ways that are in line with national needs.

How is this new form of power dispersed? A shift here is parallel to that of the direction of individualization. In the Middle Ages, individualization was concentrated at the summit, in the figure of the sovereign, while now it has trickled down to the base, to the population, since the individual members of a given population must be visible for the disciplinary society to be capable of gaining information about them. Power became anonymous, machine-like (Dosse 1998, 253). This entails a central shift in Foucault's analysis of change in power relations. Power once concentrated in the figure of the sovereign, has now become divided into numerous discursive flows, made manifest in institutions such as the asylum, the prison, the military, schools, and so on. Visibility, then, was the method used to shape modern subjectivity capable of being disciplined using certain new techniques.

2.2.1. Methods of disciplining

Following the notion of visibility, Foucault became particularly interested in how this new form of power became capable of exerting control (power) over people without such manifest exercise of force all the while being more effective than its predecessor (Guttig, Oskala

2022). He identified three main methods: hierarchical observation, normalizing judgment, and examination.

Observation became the central trait of disciplinary societies. In the past, for example, castles were built for the purpose of being seen and thus revered, while fortresses had the architecture optimized for the observation of external space – on the other hand, modern enclosed spaces are conceived as to build an internal system of control (Foucault 1995, 172). The purpose of enclosed spaces in disciplinary societies converged not in a way to produce a sort of dualism – where the purpose of architecture is to be seen but also to observe external spaces – but rather in a way that dismisses the previous border of internality and externality by making observation immanent, unavoidable. Foucault saw the prison as the model for all modern enclosed spaces in which power was dispersed – however, he also gives the example of the school and all of its "petty mechanisms" (the way supervisors' platforms were elevated to observe all the pupil's tables, the layout of dormitories, etc.) in describing the architecture of observation. The thought of being observed is enough for a subject to comply as if he was actually being watched.

The other two methods – normalizing judgment and examination – are closely intertwined and the latter in part makes the former possible. Disciplinary punishment upholds an order that is double in nature – on the one hand, it is the explicit normative rule (for example, the duration of the school curriculum), and on the other, a natural limitation (the cognitive development of a pupil at a given age). By combining these two components, one gets a picture of what is deemed normal or abnormal, thus introducing a moral component, whether something is good or bad. This is again a delineation from sovereign power, which only judges an action on the basis of whether it is prohibited. Here, punishment has not only a penal, but a normalizing component. Success is rewarded by advancement and punishment then is the opposite, regression.

Finally, through examination – present in various spheres of life, from psychiatry to schools – power structures are capable of monitoring the performance of disciplinary subjects and thereby controlling them (psychiatric evaluation, grading in schools, etc.). Based on this information, institutions create strata, grades, and norms that serve as the source of knowledge about the individual. The individual consequently becomes a "case" in the sense that he is the object of scientific

inquiry as well as something to be cared after (Foucault 1995, 170–175; Guttig, Oskala 2022). By this scientific empirical monitoring, be it medical, academic or legal – care becomes a new way of control as it is based upon the aforementioned collected data about the subject.

3. CONTEMPORARY THEORIES

Although connected to Foucault's theory, theoreticians like Deleuze and Zuboff locate the points of discipline and control in different but complementary ways, through the notion of surveillance. For Deleuze, new altered space and new technologies prove to be new ground for surveillance, while Zuboff analyzes how data is used for economic exploitation and the way that opens up a new way of surveillance (Galič, Timan, Koops 2017, 18–19). The point of this chapter is to elaborate both theories and propose a reading that suggests that surveillance capitalism is a subset of control societies that concretizes it.

3.1. Societies of Control

Building upon Foucault's schema, Deleuze (1997, 178–179) claims that we are presently witnessing another shift in the ways in which power exerts itself upon individuals. He thought of disciplinary spaces as molds – fixed and created to shape individuals. They are productive in the sense that they shape subjects. But with the advent of control societies, closed molds of institutions turned into open systems that function on the logic of modulations – that is, they adapt in accordance with changing conditions. At first, Deleuze noticed this trend in the shifting importance from the factory to the company, where the factory maintained a somewhat stable relation of production and wages, while the company, compared to the factory where there was a clear division of interests between the factory owner and its workers, stimulates constant rivalry through challenges, contests that modulate the individual, thus dissolving group interests (Deleuze 1997, 179). A transcendence is present, a duality of actuality and virtuality where there is an individual – the person as he or she is – but also a double who that individual strives to become (Moore 2009, 146). For Deleuze, then, unlike the possible, the virtual is already real – it's a part of reality, albeit ideal, but only in genesis is the virtual actualized. Therefore,

the virtual serves as grounds for anything actual and is presupposed[2]. This dualism is highly individualized and, for that reason, it becomes impossible to reassemble individuals into a traditional group (Moore 2009, 144–148).

All of this is in part a consequence of the change in material conditions where:

> "Capitalism in its present for is no longer directed toward production, which is often transferred to remote parts of the Third World, even in the case of complex operations like textile plants, steelworks and oil refineries. It's directed toward metaproduction. It no longer buys raw materials and no longer sells the finished products: it buys finished products or assembles them from parts. What it seeks to sell is services and what it seeks to buy, activities. It's a capitalism no longer directed toward production but toward products, that is, toward sales or markets" (Deleuze 1997, 181).

Here Deleuze is pointing to the fact that western capitalism has entered a new postmodern phase of production presently unique to it, which is contingent upon the existence of the so called third world through the delegation of traditional production. This does not exclude the third world from adopting trends of control societies, but it certainly widens the gap between it and the developed world, something that will be important for our further analysis of data protection.

A major shift was the analysis of open spaces instead of enclosed spaces in disciplinary societies. Before, an individual always started all over (from school, to the barracks, to the factory...), but that is no longer the case, since the individual is never finished with anything, but is in a constant state of development (Deleuze 1997, 180). As a result, the outside has now become confined. Before, enclosed spaces served the purpose of picking out one possibility out of infinite virtualities. Disciplinary institutions thus were not only repressive but also productive, since they chose the actual from the virtual. Deleuze claims that what is confined now is the virtual itself, and that is done through its periodic regulation and capture (Lazzarato 2009, 175–178).

From here, we see that the group has dissolved first into individuals, but for Deleuze, this is only a stepping stone. In disciplinary societies, Foucault located two poles, "the signature that designates the

[2] See also: Stanford Encyclopedia of Philosophy, 2022b.

individual, and the number or administrative numeration that indicates his or her position within a mass. This is because the disciplines never saw any incompatibility between these two and because at the same time, power individualizes and masses together, that is, constitutes those over whom it exercises power into a body and molds the individuality of each member of that body" (Deleuze 1997, 179–180). Here, the fact stressed is the importance of the mass (group) in shaping individual subjectivity, and vice versa. The corporation does not strive to achieve that level of control but rather seeks to manage only specific parts of the market that it pertains to. Due to the modulating nature of the social institutions, individuals have become less stable as a category, since their utility changes with the shifting nature of said institutions. As he (Deleuze 1997, 180). continues, "in the societies of control, on the other hand, what is important is no longer either a signature or a number, but a code: the code is a password". It is no longer individuals as a whole who play a pivotal role in interacting with different social systems, but rather only the individual's "representation", their behavior as a consumer. To explain this fragmentation of the individual, Deleuze coined the term "dividual" (Galič, Timan, Koops 2017, 19–20).

Using Deleuzes tools, Haggarty and Ericson (2000, 611) write of the body as the object of abstraction from its physical form, which is then it is reassembled in various new "data flows", a data double that is essentially virtual. The body is diffused into a multiplicity of "discrete signifying flows" (Haggerty, Ericson 2000, 612). Next, these flows of information, after becoming detached from corporeality itself, become "pure information", independent and ready for processing. This processing is done in "centers of calculation" which can include "forensic laboratories, statistical institutions, police stations, financial institutions, and corporate and military headquarters". Data doubles, according to them, permeate various centers of calculation, and are used for accessing resources and services in ways increasingly unbeknown to the individual, with the trend of increasing their use for marketing purposes (Haggerty, Ericson 2000, 613).

A dividual then is a different source of information depending on the institution you're interacting with. For example, to the bank, you are your credit score; to an insurance agency, you are a combination of your risk factors that determine the height of the premium you have to pay; to the police, you are your criminal record; on social media, you

are your preferences deduced from the type of content you consume, etc. The individual is turned into a multiplicity of data-banks.

3.2 Surveillance capitalism

To meaningfully develop the general theory put forth by Deleuze, one must introduce another idea. The American sociologist and philosopher Shoshana Zuboff was the one to fledge out the notion of surveillance capitalism first. She defines it as a new subset of information capitalism whose primary goal is to "... predict and modify human behavior as a means to produce revenue and market control" (Zuboff 2015, 75). The process initially stared developing with Google, but was perfected with Facebook. However, now it cannot be even identified with a single company as it has become entrenched in almost all internet activities. Digital technology (algorithms, sensors, machine intelligence, platforms etc.) is not to be understood as a dependent constituent of surveillance capitalism, as technology can exist without an economic creation (surveillance capitalism) while the reverse is not possible, but in that relation the economic component always has the primate over the technological one (Zuboff 2019, 12–13).

However, the notion of "big data", Zuboff claims, is not just some "autonomous process" of digital technologies, but an immanent part and the object of commodification within the system of surveillance capitalism. With the spread of computer mediation in various spheres of social life, many of our actions have become visible and accessible. But the important questions are to whom is this data visible and who decides what is accessible. Zuboff uses as a starting point for her analysis two documents written by Google's Chief Economist Hal Varian (Varian 2010, 2014). as a starting point of her analysis. Unlike her, Varian sees potential for human development in big data. By claiming that "computer-mediated economic transactions" get recorded and thus help improve future interactions, Varian, Zuboff (2015, 76–78) argues, entails an important aspect of big data, and that is that it subverts an important aspect of the neoliberal market – that it is unknowable. From there, building on Varian's four new uses implied by computer-mediated transactions, Zuboff contours the ways new capital accumulation is performed:

1. Data extraction and analysis. One of the main components of surveillance capitalism is its appetite for data collection and

analysis (data analysis), from which two characteristics can be deduced:

a) Formal indifference is the consequence of the asymmetry between the persons from whom the data is extracted, and the market actors (social media companies for example) who do the extracting of said data;
b) Structural independence signifies the fact that there are no reciprocities between the company and the population. For example, there are increasingly less durable employment systems, steady wage increases, etc. As a consequence, companies like Google are capable of creating enormous revenue with a relatively small workforce due to the fact that they primarily use algorithms to deal with other actors such as advertisers.

2. New contractual forms due to better monitoring. Real-time monitoring of contractual performance, people create a large quantity of data that is apt for monitoring, observation, and finally manipulating establishing conditions that increase control.
3. Personalization and communication. This characteristic refers to the way algorithms predict what the individual wants and needs to know even before the individuals knows it themselves.
4. Continuous experiments. Since big data analysis yields only correlational patterns, constant experimentation is necessary to expose causality. For example, Facebook continually does this by manipulating its users' behavior for the sake of monetization (Zuboff 2015, 78–85).

3.3. Connecting the two theories

How is this conception of surveillance capitalism connected to Deleuze? In our opinion, these two theories converge in three major ways. Those can be divided into relations concerning the subject of surveillance, the change in the frontier of control and in terms of the object of control.

First, in terms of the main actor in the new architecture of surveillance, both Zuboff and Deleuze agree that private enterprise has the primate over the state, and that state power is to be understood separately. As already stated, the interests of the company are drastically different in scope to the interests of the state and, therefore, they

rarely contradict each other, leaving space for the development of parallel forms of control.

Secondly, the change in the frontier of control is in both theories moved to the enclosure of the outside, or what was perceived to be out of the purview of control in the past. For Zuboff, that is overcoming the unknowability of the market which used to be postulated by neoliberal theory, and for Deleuze, with the breaking down of disciplinary institutions that served the purpose of channeling the virtual into a specific mold, now the virtual itself becomes regulated from a distance. For this Deleuze gave the example of how highways give the impression of freedom of movement, all the while posing as another form of control (Deleuze 2006, 322). The perception of freedom in the middle of monitoring is the dominant logic of control societies.

Thirdly, and most importantly, when it comes to the object of control/surveillance, for one to arrive to Zuboff through Deleuze, one must connect them through more recent interpretations. Since Deleuze wrote about control societies in the early stages of computerization he couldn't anticipate the impact information technology would have in this field. Therefore, one must expand his concepts so that they can be applicable for the modern day. Clarke (1988, 449) coined the term "dataveillance" to explain "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons". Dataveillance differs from panoptic ways of control in that it is far more efficient, since it utilizes digital instead of analog technology. If we consider the vast systematizing ability of digital databases as well as their quantitative abilities, one can see how the connection with the digital has been made with the aforementioned concept of the dividual. Data, through the spreading of the internet and social media, has become increasingly available to a greater number of data collectors, instilling a sense of increased uncertainty (Galič, Timan, Koops 2017, 28). If we take this interpretation of Deleuze, we believe that Zuboff's theory fits neatly within the framework of societies of control.

4. THE EUROPEAN UNION AND DATA PROTECTION

Since the before explained trends are not universal, but develop non-linearly in different regions of the world, and taking into consideration the fact that this asymmetry is in some sense inherent since the

West shifted toward "higher-order" production emblematic of control societies only after displacing the production of raw materials to the developing countries, we will focus on the way big data has been regulated in said developed countries. Specifically, attention will be devoted to the most recent attempt at protecting data – that is, the European Union General Data Protection Regulation (GDPR).

In 2016 the European Union (EU) passed the GDPR, which came into force in 2018, thus replacing the Data Protection Directive (DPD)[3] from 1995. This update in data regulation came to pass due to the rapid advancement in technology making the DPD outdated[4].

4.1. Big data and the European Union

Although there isn't a definition of big data included within the GDPR itself, a year after its passing, the European Parliament passed a resolution that defined it as "the collection, analysis and the recurring accumulation of large amounts of data, including personal data, from a variety of sources, which are subject to automatic processing by computer algorithms and advanced data-processing techniques using both stored and streamed data to generate certain correlations, trends, and patterns (big data analytics)"[5].

From this definition, a few points can be made about big data: Firstly, it usually but not always encompass personal data; the quality of the data is not all that important, but it's the quantity that counts; very importantly, due to the vast quantity of data, algorithms attempt to structure them and locate regularities; regardless of the intent to use it, all sources of data must be analyzed separately; a general formula can be inferred: the more data there is, the more precise the results; the results are never a consequence of only one data point but of a network of data. Because most of this data is unstructured, it is difficult to find

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995.

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

[5] Resolution (2016/2225(INI)) of the European Parliament of 14 March 2017 on fundamental rights implications of big data: privacy, data protection, non-discrimination, security and law-enforcement, OJ C 263 of 25.7.2018.

a genealogy of big data analysis due to its dispersed points of origin. It is therefore difficult to bind the purpose of data extraction and consent for its use, which is the greatest difficulty of data protection (Galič, Timan, Koops 2017, 61–63).

Most importantly, despite its quantity, the defining characteristic of big data is its ability to systematize said data for the sake of making precise prediction about the future behavior of users (Andrew, Baker 2021, 566), which is what Zuboff meant when talking about personalization and communication. This relation of yielding private data for the sake of gaining something in return is not balanced, since companies like Facebook and Google are not held accountable the same way traditional institutions can be. The users are quite oblivious to the ways their data is used for by these companies (Zuboff 2015, 83).

Deleuze pointed out in the already mentioned seminar that control societies no longer pass through places of confinement. By breaking down the boundaries of institutions, various previous spheres of life converge on each other. Control is not the same as discipline. Control, after it leaves the premises of confinement is seamless. Movement can seem free, but it is controlled at the same time (Deleuze 2006, 321–322). This is exactly what happens with big data. This is evident since human behavior is monitored through mundane activities such as going to the supermarket, online transactions, google searches, movement etc. (Andrew, Baker 2021, 567). Therefore, movement and consumption are encouraged because said activities increase the amount of data that can be collected and used for analysis.

4.2. Impact of the General Data Protection Regulation

Following the analysis of big data, the GDPR implicitly regulates a specific subset of big data pertaining to personal data through the notion of profiling. Profiling is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements"[6]. The GDPR prohibits automated processing, including profiling and establishes a

[6] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of

system of explicit consent.[7] However, there are enumerated exceptions to this rule, namely, the prohibition of automated processing, including profiling shall not apply if it "is necessary for entering into, or performance of, a contract between the data subject and a data controller"[8]. This is an improvement compared to the DPD[9] in the sense that an explicit necessity criterion is introduced. The problem is that this concept is not elaborated within the text of the regulation itself, so it will probably be fleshed out in the still undeveloped practice of the courts. In another respect, this exception is expanded. The DPD required the data subjects to explicitly request the contract, while now the exception includes the contracts the controller requests (Bygrave 2020, 536).

However, one is reminded of Zuboff's analysis of the role of the contract in her theoretical framework. Varian gave some dystopian suggestions of how contracts can, through computer-mediated transactions, facilitate new relations. He talked of how insurance companies could use monitoring systems to check if the customers are driving safely in order to determine if they want to continue providing the insurance. For Zuboff (2015, 81–82) this is the antithesis of the classical notion of the contract and the rule of law as "consensual participation", she writes, "in the values from which legitimate authority is derived, along with the free will and reciprocal rights and obligations, are traded in for the universal equivalent of the prisoner's electronic ankle bracelet". The contract has become a method of forfeiting privacy for something in return such as "a mortgage, medical advice, legal advice – or advice from your personal digital assistant" (Varian 2014, 30).

Another point of contention is the GDPR's introduction of de-identified data sets, namely anonymized[10] and pseudonymized data[11].

---

personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119 of 4.5.2016, Article 4(4).

[7] *Ibid*., Article 22 paragraph 1.

[8] *Ibid*., Article 22 paragraph 2 item (a).

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995, Article 15 paragraph 2 item (a).

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ* L 119 of 4.5.2016, recital 26.

[11] *Ibid*., Article 4, paragraph 5.

The main difference between them is whether the data subject can none the less be reidentified at the end (Andrew, Baker 2021, 71–72). So, when it comes to anonymized data, this cannot be done, while in the case of pseudonymized data this is possible with the help of additional information. This, even though it is a step in the right direction, can prove to be another place for manipulation, especially if we consider the fact that anonymized data, which offers a more robust type of protection, is regulated in a recital, while pseudonymized data is set in an article of the regulation.

In order to propose another shortcoming of the GDPR, one must understand the conceptual distinction between privacy and surveillance risks. The former is concerned with the individual, it sheds light on the individual's right to protect his private information – it preserves the subject (Andrew, Baker 2021, 69), while the latter differs in scale and is connected with the problems controlling and governing the trade of personal data. Also, importantly, data surveillance does not need personal data for analyzing anonymized data sets. From the vast quantity of this data, personal data can be inferred (Andrew, Baker 2021, 71).

The GDPR, through prioritizing privacy risk in paragraph 26[12] by stating that the principles of data protection should pertain to information concerning an identified or identifiable person, incentivizes the collection of other de identified behavioral data, which, as stated before, can all the same be used for reconstructing behavior. Something which has been done by large companies such as Facebooks and Google for a long time (Andrew, Baker 2021, 74). In a way, by excessively affirming subjectivity through the protection of private data, the GDPR can have an effect of destabilizing it further, which brings us back to the notion of control societies. By stimulating the anonymous flows of information constituting the aforementioned data double, a pure virtuality that all the same can be used to shape our behavior as postulated by Zuboff, the GDPR missed the opportunity to protect data subjects from surveillance risks.

At this moment, only a few years after the coming into force of the GDPR, it is still too early to say if and what effect this will have

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ* L 119 of 4.5.2016, paragraph 26.

on the big data industry, but some signs might have already started to manifest. Zarsky (2016, 1018) proposes some scenarios for how the GDPR might affect data protection. First, the optimistic scenario is that the GDPR fulfills its ostensive purpose in safeguarding fundamental privacy rights. The idea is that citizens themselves will enjoy enhanced data protection, all the while experiencing the benefits of data analysis. There have already been some such indications – for example, a study conducted in the Netherlands, suggests that the GDPR had minimal effects on e-commerce companies, and that their business operated uninterrupted in spite of previously pessimistic forecasts. The study even suggests that the implementation of the GDPR enhanced data management within companies and increased customers' trust (Haddara, Salazar, Langseth 2023, 776). Also, there is the prospect of globalization of these rules due to GDPR's international jurisdiction, which opens the possibility of its use outside the EU, most importantly in the US. However, due to the fact that there are many situations of data analysis that the GDPR does not regulate or does so vaguely, which is why many call it "sluggish" (Diligenski, Prlja, Celović 2018, 17), there is a possibility that different EU countries will implement this regulation differently, for better or for worse (Zarsky 2016, 1019). Finally, the moderate forecast of its rules is that it will, due to its framework nature, provide enough wiggle room for data analysis companies to continue developing (Zarsky 2016, 1019).

5. CONCLUSION

The largest change that was observed in the shift from disciplinary to control societies was in the notion of the subject who is no longer the object of discipline which in large part shaped it, but rather has become an object of monitoring. The nature of this new subjectivity was examined, and the notion of the fragmented data double was introduced, so that it could be used for the further exploration of questionable data analysis that threatens fundamental rights and its attempts at curbing them.

The main takeaway from the theoretical part of the paper is that both the concepts of control societies and surveillance capitalism are relevant to the present and that they are in a relation of subordination. Surveillance capitalism can be viewed as a subset of control societies

and, being a narrower term, it can be efficiently used for the dissection of the trends of big data analysis as both a method by which data is commoditized and subjects are controlled.

Even though the GDPR provides unprecedented protection of private data, even after a short period after its coming into force concerns have been raised in theory. The first among them is the difficulty to bind the purpose of data extraction and consent for its use, so that it can be meaningfully protected. Also, in its attempt to mitigate privacy concerns, the GDPR might inadvertently incentivize the increased harvesting of behavioral data, which in turn could be a fertile ground for future behavior manipulation of users both online and offline. Another concern is that the implementation of the regulation might vary in quality and robustness among the 27 EU nations, which would further destabilize its utility. These critiques, as well as some others, on their own might be minimized, but taken together they make it seem increasingly likely that the GDPR won't have the power to meaningfully challenge interests of the emerging economic order.

The given analysis of the GDPR contributes to the picture of a crumbling notion of Foucault's disciplinary subject, which is becoming increasingly obscure and fragmented into a multiplicity of data flows. These, in turn, are used to predict and manipulate the behavior of said subject in spite of the ostensible attempts at protecting it, such as the one offered by this regulation.

All in all, given the fact that the trends of commoditization and of flows of data in control societies have proven to be immensely profitable, it seems unlikely that any number of lawsuits or new regulations would entirely undermine this new logic of accumulation, since abandoning it would mean the end of the present mode of capital accumulation. This outcome seems even more plausible when paired with the conclusion about the capabilities of the GDPR.

REFERENCE LIST

1. Andrew, Jane, Max Baker. 3/2021. The General Data Protection Regulation in the Age of Surveillance Capitalism. *Journal of Business ethics,* 168: 565–578.
2. Bygrave, Lee A. 2020. Article 22. Automated individual decision-making, including profiling. 522–543 in *The EU General Data Protection Regula-*

tion (GDPR): A commentary, edited by Christopher Kunder, Lee A. Bygrave, Christopher Docksey. Oxford: Oxford University press.

3. Clarke, Roger A. 5/1988. Information technology and dataveillance. *Communications of the ACM,* Vol. 31: 498–512.
4. Deleuze, Gilles. 1988. *Foucault*. Minneapolis: University of Minnesota Press.
5. Deleuze, Gilles. 1997. *Negotiations 1972–1990*. New York: Columbia University Press.
6. Deleuze, Gilles. 2006. *Two Regimes of Madness: Texts and Interviews 1975–1995.* New York, Los Angeles: Semiotext(e).
7. Diligenski, Andrej, Dragan Prlja, Dražen Cerović. 2018. *Pravo zaštite podataka: GDPR*. Beograd: Institut za uporedno pravo Beograd.
8. Dosse, Francois. 1998. *History of Structuralism Vol. 2.* Minneapolis: University of Minnesota Press.
9. Foucault, Michel. 1976. *The History of Sexuality Vol 1: An Introduction.* New York: Pantheon Books.
10. Foucault, Michel. 1995. *Discipline and punish.* New York: Vintage books.
11. Galič, Maša, Tjerk Timan, Bert-Jaap Koops. 1/2017. Bentham, Deleuze, and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy and technology*, Vol. 30: 9–37.
12. Haggerty, Kevin D., Richard V. Ericson. 4/2000. The surveillant assemblage. *British Journal of Sociology*, Vol 51: 605–622.
13. Haddara, Moutaz, A Salazar, Marius Langseth. 2023. Exploring the Impact of GDPR on Big Data Analytics Operations in the E-Commerce Industry. *Procedia Computer Science*, Vol. 219: 767–777.
14. Lazzarato, Maurizio. 2009. The Concepts of Life and the Living in the Societies of Control. *Deleuze connections: Deleuze and the Social:* 171–191
15. Moore, Nathan. 2009. The Perception of the Middle. *Deleuze connections: Deleuze and Law:* 132–150.
16. Niče, Fridrih. 1990. *Genealogija morala.* Beograd: Grafos.
17. Protevi, John. 2009. The Terri Schiavo Case: Biopolitics, Biopower, and Privacy as Singularity. *Deleuze and Law: forensic futures*: 59–72.
18. Stanford Encyclopedia of Philosophy. 2022a. Michel Foucault. *https://plato.stanford.edu/entries/foucault/* (last visited 14 October, 2023).
19. Stanford Encyclopedia of Philosophy. 2022b. Gilles Deleuze. *https://plato.stanford.edu/entries/deleuze/* (last visited 25 January, 2024).
20. Varian, Hal R. 2/2010. Computer Mediated Transactions. *American Economic Review,* Vol. 100: 1–10.
21. Varian, Hal R. 1/2014. Beyond Big Data. *Business Economics,* Vol. 49: 27–31

22. Zarsky, Tal. 4(2)/2016. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47: 995–1020.
23. Zuboff, Shoshana. 1/2015. Big Other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology,* 30: 75–89.
24. Zuboff, Shoshana. 1/2015. Surveillance Capitalism and the Challenge of Collective Action. *New Labour Forum*, Vol. 28: 10–28.

UDK 342.738:004.738.5
DOI 10.51204/IVRS_24105A

Marija Vojisavljević*

EVROPSKA REGULACIJA ZAŠTITE PODATAKA NA INTERNETU

Pravo na privatnost je posebno ugroženo pojavom novih informacionih tehnologija. U vremenu koje karakteriše obrada ogromne količine najrazličitijih podataka, tzv. eri velikih podataka, lični podaci se tretiraju kao najznačajniji resurs. Internet je omogućio pristupanje podacima koji se mogu zloupotrebiti. Prepoznajući opasnosti koje internet sobom nosi, članice Evropske unije su preduzele brojne značajne aktivnosti sa ciljem da se zaštite prava korisnika interneta i da im obezbede sigurnost na mrežama. U ovom radu su predstavljene odredbe i principi zaštite podataka o ličnosti i privatnosti na internetu sadržane u Evropskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda, Direktivi 95/46, Povelji Evropske unije o osnovnim pravima, Direktivi 2002/58, Direktivi 2016/680 i Uredbi 2016/679. Konvencije, uredbe i direktive se razmatraju da bi se utvrdilo u kojoj je meri Evropska unija uspela u svojoj nameri na pronađe adekvatnu pravnu regulativu zaštite podataka na internetu.

Ključne reči: *internet, onlajn pretnje, podatak o ličnosti, pravni akti Evropske unije, privatnost*

1. UVOD

Internet je revolucionarni pronalazak čije žile prodiru u gotovo sve sfere čovekovog postojanja i rada (Šarkić *et al*. 2007, 120). U svetu koji se menja neverovatnim tempom, tehnološke inovacije dešavaju nam se pred očima. Kako tehnologija napreduje, često se zapitamo kako smo uopšte živeli bez telefona, tableta, interneta. Kako smo ispunjavali dane, noći, vikende (Kol 2021, 15)?

* Autorka je studentkinja osnovnih akademskih studija na Pravnom fakultetu Univerziteta u Beogradu, *marijavojisavljevic2003@gmail.com*.

Život u 21. veku nezamisliv je bez tehnologije i interneta. Svojom pojavom internet je doneo brojne pogodnosti koje su olakšale odvijanje svakodnevnog života. Čovek ga koristi da uči, da se zabavlja, trguje, kupuje, traži ili nudi zaposlenje, pa čak i da obavlja svoje redovne poslove (Šarkić *et al*. 2007, 120). Sve informacije su nam na dohvat ruke, možemo komunicirati sa bilo kim na svetu, a virtuelni svet je postao sastavni deo našeg stvarnog života. Nema više gledanja sporog učitavanja podataka, lutanja po bibliotekama kako bismo pronašli neku informaciju, slanja pisama... Sada većinu problema rešavamo kod kuće, uz pomoć nekoliko klikova.

Istovremeno, ljudi uglavnom nisu svesni svih negativnih strana interneta i često sami sebe nepromišljeno čine lakom metom raznih zloupotreba. Danas pojedinac, šta god da uradi, bilo da se tiče njegovog poslovnog, porodičnog ili ljubavnog života, ne može a da to ne podeli sa svima putem društvenih mreža i sav sadržaj podeljen putem interneta postaje lako dostupan svima. Privatnost na internetu jedva da postoji i u najvećem broju slučajeva mi smo ti koji je narušavamo svojim neodgovornim ponašanjem (Milovanović 2019). Korisnici društvenih mreža najčešće ne razmatraju opasnost zloupotrebe ostavljenih podataka i olako smatraju da nisu ugroženi.

Na taj način mreže postaju jedinstvene socijalne platforme sa velikom bazom razmene ličnih podataka. Nesmotrenost na mrežama uzrokovala je mnoge incidente širokog spektra, što je uticalo da internet korisnici počnu da izražavaju zabrinutost zbog značajnog objavljivanja i korišćenja njihovih ličnih podataka (Acquisti, Gross 2006). Lični podaci se često distribuiraju bez znanja korisnika, dok fotografije mogu da se iskoriste ne samo za zlonamerna prikazivanja već i za prepoznavanje lica, što je posebno interesantno državnim organima (Baltezarević 2015, 243). Zbog korišćenja moderne tehnologije živimo u potpuno povezanom svetu, u kome skoro svaki potez ostavlja digitalni trag. Lako je navići se na nove funkcionalnosti, ali takođe moramo da razmotrimo i opasnosti koje idu podruku sa tehnološkim napretkom, a još važnije je da pronađemo način kako da se od njih zaštitimo (Kol 2021, 7).

Cilj ovog rada je da istražimo traganje Evrope za adekvatnom pravnom regulativom zaštite podataka na internetu. Osim toga, u radu će biti obrađene i teme koje se tiču toga na koje sve načine ostavljamo podatke na internetu, kao i pitanje njihove zloupotrebe.

2. PRIVATNOST NA INTERNETU – ONLAJN PRETNJE

Privatnost se načelno može definisati kao pravo nekog lica da određeni krug podataka i informacija koje se na njega odnose sakrije od oka javnosti. Još je Aristotel u delu *Politika* istakao razliku između javne i privatne sfere. Prva se odnosi na organizaciju države i života u njoj, pa je samim tim od opšteg značaja, a potonja se vezuje za lični i porodični život, pa se tiče pojedinca ili grupe pojedinaca, a ne društva u celini. Kako su se, u narednim vekovima, sve više razvijale političke, društvene i ekonomske prilike, razvijao se i koncept privatnosti. Važno je istaći da opštu evoluciju koncepta privatnosti karakterišu i uspostavljanje i izgradnja tzv. prava na privatnost. Prepoznavanje i priznavanje prava na privatnost nastalo je iz potrebe da se obezbede što efikasniji mehanizmi zaštite privatnosti jer su, sa društvenim i tehnološkim napretkom, mogućnosti njene povrede postale sve dostupnije.

Jedan od lako dostupnih instrumenata pomoću kojeg se može povrediti pravo na privatnost jeste i internet (Popović, Jovanović 2017, 123). Internet je omogućio praćenje komunikacija, analizu fotografija, pristupanje ličnim podacima korisnika i njihovo dalje distribuiranje, bez saglasnosti i znanja osobe čiji su podaci. Otkrivanjem ličnih podataka korisnici sami doprinose stvaranju digitalnih zapisa o njima. Tako ostavljene informacije i podaci sa korisničkog profila mogu biti zloupotrebljeni na različite načine. Podaci mogu da se iskoriste za pričinjavanje štete korisnicima i eventualnu ucenu, krađu identiteta, sajber nasilje i slične oblike zloupotrebe (Baltezarović 2017, 244). U vremenu koje karakteriše obrada ogromne količine najrazličitijih podataka, tzv. eri velikih podataka, lični podaci se tretiraju kao resurs. Svoje „besplatne" usluge kompanije naplaćuju korisnicima tako što za uzvrat traže sve više ličnih podataka. Podaci o korisnicima, njihovim aktivnostima i ponašanju na internetu koriste se za analizu i kreiranje ličnih socijalno-psiholoških profila, ciljano plasiranje komercijalnih proizvoda prilagođenih individualnim karakteristikama i potrebama korisnika, za prodaju kompanijama ili servisima. (Kuzmanović 2019, *https://digitalni-vodic.ucpd.rs/ zastita-licnih-podataka-i-privatnosti-na-internetu/?lng=lat*). Dakle, koliko god da je okolnost da su od svega udaljeni „samo jedan klik" ljudima učinila život lakšim i udobnijim, toliko ih je i izložila riziku da njihovi lični podaci i privatne informacije lako završe kod onih kojima nisu namenjeni. Da bi se stekla slika

o dostupnosti podataka i ugroženosti privatnosti na internetu, dovoljno je setiti se samo nekoliko poznatih, relativno novijih slučajeva. U julu 2017. godine u Švedskoj je izbio skandal kada se saznalo da je dve godine ranije švedska transportna agencija na jedan klaud server postavila, a zatim greškom elektronskom poštom neovlašćenim licima poslala baze podataka sa imenima, fotografijama i kućnim adresama miliona švedskih državljana, uključujući i pripadnike tajnih jedinica policije i vojske, učesnika programa zaštite svedoka...[1] U maju 2014. godine čuvena plaforma za kupovinu putem interneta *eBay* objavila je da je bila žrtva hakerskog napada usmerenog na preuzimanje imena, adresa, datuma rođenja i kriptozaštićenih lozinki oko 145 miliona korisnika ove platforme.

Svemu tome treba dodati i rizike kojima se korisnici interneta ponekad sami izlažu nedovoljno pažljivim skladištenjem podataka na udaljenim serverima ili postavljanjem ličnih, odnosno privatnih informacija na raznim društvenim mrežama (Popović, Jovanović 2017, 123–124). Privatnost korisnika, na primer, na Fejsbuku, narušena je samom objavom bilo kojih informacija na toj društvenoj mreži. Te informacije automatski pripadaju toj kompaniji i ostaju sačuvane u njihovim serverima, čak i u slučaju gašenja naloga. Da bi se kreirao nalog na toj, kao i na ostalim društvenim mrežama, korisnik mora da navede svoje ime, e-adresu, datum rođenja i pol i one spadaju u javno dostupne informacije. Osim navedenih, u javno dostupne informacije spadaju i profilna slika, mreža, korisničko ime i korisnički ID i te informacije su dostupne svima na internetu. Te informacije mogu biti zloupotrebljene i korisnik može biti izložen riziku od krađe identiteta. Krađa identiteta najčešće je zločin za finansijsku dobit.

Takođe, kada korisnik objavi fotografiju ili video-zapis, to omogućava i dobijanje dodatnih podataka poput vremena, datuma i mesta fotografisanja ili pravljenja video-zapisa. Podaci se prikupljaju i sa računara, mobilnog telefona ili nekog drugog uređaja posredstvom koga se pristupa internetu. U te podatke mogu da spadaju lokacija, vrsta pretraživača ili stranice koje korisnici posećuju. Zanimljivo je i to da se na većini sajtova društvenih mreža od korisnika zahteva da prihvate polisu o uslovima korišćenja, pre nego što mu dopuste da koriste njihove usluge. Kontroverzno je to što polisa o uslovima korišćenja koju korisnik mora da prihvati često sadrži klauzule koje

[1] Više o tome: Khandelwal Swati, Sweden Accidentally Leaks Personal Details of Nearly All Citizens 2017. *https://thehackernews.com/2017/07/sweden-data-breach.html*.

dozvoljavaju operatorima društvenih mreža da skladište podatke o korisnicima, ili da ih čak dele trećim licima, najčešće marketinškim kompanijama. U većini slučajeva, polise su koncipirane tako da su za korisnika nerazumljive i preobimne, pa ih najčešće prihvata i ne čitajući ih (Popović 2016, 37–41).

Svi ti rizici, koji ne iscrpljuju sve opasnosti po lične podatke i privatnost sa kojima se korisnici interneta susreću prilikom gotovo svakog korišćenja svetske mreže, dovoljno upečatljivo ukazuju na potrebu uspostavljanja i razvoja instrumenata i mehanizama pravne zaštite podataka o ličnosti i privatnosti na internetu, što će biti tema u nastavku rada (Popović, Jovanović 2017, 124).

3. EVROPSKA REGULACIJA ZAŠTITE PODATAKA NA INTERNETU

Trenutno važeći pravni okvir zaštite podataka o ličnosti[2] u pravu Evropske unije (EU) rezultat je višedecenijske evolucije.

Prvi implus za izgradnju tog pravnog okvira došao je spolja. Organizacija za ekonomsku saradnju i razvoj je 1980. godine usvojila *Preporuke o smernicama za zaštitu privatnosti i prekogranični protok ličnih podataka.* Smernice nisu imale pravno obavezujući karakter, tako da nisu u značajnijoj meri doprinele harmonizaciji pravnog okvira za zaštitu ličnih podataka u državama članicama Organizacije. Nešto značajniji korak učinjen je godinu dana kasnije – 1981. godine, kada je pod okriljem Saveta Evrope sačinjena Konvencija o zaštiti lica u odnosu na automatsku obradu podataka. Predlagač Konvencije je imao nameru da zemlje potpisnice usklade svoja nacionalna zakonodavstva sa osnovnim načelima i preporukama sadržanim u ovom dokumentu. Poštujući vladavinu prava, ljudska prava i osnovne slobode, cilj Konvencije je bio da poveže svoje članice, da proširi zaštitu osnovnih prava i sloboda pojedinca, naročito njegovog prava na privatnost prilikom automatske obrade njegovih ličnih podataka (Bosnić 1998, 27). Konvenciji, koja je stupila na snagu 1985. godine, brzo su pristupile i neke države članice (tadašnje) Evropske ekonomske zajednice (EEZ), pa se

[2] Podatak o ličnosti je svaki podatak o čoveku. To može biti, na primer, podatak o imenu lica, adresi, sedištu, broju telefona, podatak o obrazovanju, podatak o zaradi, podatak o imovini, podatak o nacionalnoj pripadnosti, podatak o bolesti od koje se leči.

očekivalo da će u kratkom roku sve države članice iskazati saglasnost na obavezanost Konvencijom. Kako se to za prvih pet godina važenja konvencije nije desilo, Evropska komisija je pristupila izradi direktive kojom bi se osnovna pitanja zaštite podataka na jednoobrazan način uredila u EEZ. Poduhvat Evropske komisije je okončan 1995. godine usvajanjem Direktive 95/46. Nešto više od jedne decenije kasnije, Savet EU je doneo Okvirnu odluku 2008/977/JHA o zaštiti podataka o ličnosti obrađenih u okviru policijske i pravosudne saradnje u krivičnim stvarima, kojom se nastojala postići minimalna harmonizacija propisa u oblasti zaštite podataka koji su se ticali tadašnjeg tzv. trećeg stuba EU.[3] Evolucija pravnog okvira za zaštitu podataka nastavljena je i nakon stupanja na snagu Lisabonskog sporazuma nedavnim usvajanjem Uredbe 2016/679, koja će zameniti Direktivu 95/46, i Direktive 2016/680, koja će zameniti Okvirnu odluku 2008/977/JHA (Popović, Jovanović 2017, 130–131).

U nastavku rada predstavićemo odredbe i principe zaštite podataka o ličnosti i privatnosti na internetu sadržane u Evropskoj konvenciji za zaštitu ljudskih prava i osnovnih sloboda, Direktivi 95/46, Povelji EU o osnovnim pravima, Direktivi 2002/58, Direktivi 2016/680 i Uredbi 2016/679.

3.1. Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda

Evropska konvencija za zaštitu ljudskih prava i osnovnih sloboda (EKLJP) jeste međunarodni ugovor donet pod okriljem Saveta Evrope 4. novembra 1950. godine i kasnije sukcesivno menjan i dopunjavan protokolima, koji čine sastavni deo Konvencije. EKLJP je doneta po ugledu na Univerzalnu deklaraciju o pravima čoveka iz 1948. godine, koju je usvojila Generalna skupština Ujedinjenih nacija. EKLJP je stupila na snagu 1953. godine i obavezuje sve članice Saveta Evrope. Nadzor i kontrola nad sprovođenjem EKLJP i njenih protokola u nadležnosti su Evropskog suda za ljudska prava.[4] Nacrt konvencije Saveta

[3] Evropsku uniju čine tzv. tri stuba. Prvi stub čine tri međunarodne organizacije (Evropska zajednica za ugalj i čelik, Evropska ekonomska zajednica i Evropska zajednica za atomsku energiju). Drugi stub predstavlja zajednička spoljna i bezbednosna politika EU, dok treći stub čine policijska i pravosudna saradnja u krivičnim stvarima.

[4] Evropski sud za ljudska prava je međunarodni sud sa sedištem u Strazburu. Broj sudija je jednak broju zemalja članica Saveta Evrope koje su ratifikovale Konvenciju o zaštiti ljudskih prava i osnovnih sloboda. Sudije Evropskog suda za ljudska prava

Evrope težio je tome da se postigne da obrada ličnih podataka zadovolji određeni minimalni standard ispravnosti i zakonitosti obrade, da građani dobiju mogućnost da se obaveste o obrađivanim podacima i da mogu da traže njihovu ispravku i neke druge intervencije. Formulisana su načela zaštite podataka, među kojima su i sledeća: da se lični podaci smeju obrađivati samo u svrhe za koje su prikupljeni, da se smeju obrađivati samo dok za tim postoji potreba, da podaci moraju da budu ažurirani, da svako ima pravo da bude obavešten o podacima koji se obrađuju (Šarkić *et al.* 2007, 153).

Pravni osnov za jemstvo zaštite podataka i privatnosti na internetu sadržan je u članu 8 EKLJP. Ta odredba nosi naziv „Pravo na poštovanje privatnog i porodičnog života" i ona garantuje da svako ima pravo na poštovanje svog privatnog i porodičnog života, doma i prepiske (st. 1) i da se javne vlasti neće mešati u vršenje tog prava, sem ako to nije u skladu sa zakonom i neophodno u demokratskom društvu u interesu nacionalne bezbednosti, javne bezbednosti ili ekonomske dobrobiti zemlje, radi sprečavanja nereda ili kriminala, zaštite zdravlja ili korala ili radi zaštite prava i sloboda drugih (st. 2).

Možemo primetiti da se u samoj odredba člana 8 EKLJP ne pominje eksplicitno zaštita privatnosti na internetu. Norma je formulisana na opšti način, pa je upravo takva opšta formulacija omogućila EKLJP da, u skladu sa tehnološkim napretkom evropskog društva, pod domašaj te odredbe podvede i povrede prava na privatnost koje se dešavaju na internetu.

3.2. Direktiva 95/46

Direktiva[5] o zaštiti lica u odnosu na obradu ličnih podataka i slobodnom prometu tih podataka (Direktiva 95/46) usvojena je 1995.

deluju samostalno i ne predstavljaju nijednu zemlju, mada svaka država ima po jednog člana koji je izabran od Parlamentarne skupštine Saveta Evrope. U radu sa predstavkama sud sarađuje sa Sekretarijatom, koji uglavnom čine pravnici iz zemalja članica. Oni su takođe potpuno nezavisni od naloga svojih država i ne smeju da predstavljaju podnosioce predstavki. Sud primenjuje EKLJP. Njegov zadatak je da obezbedi da države članice poštuju pravila koja su navedena u konvenciji. On to sprovodi tako što razmatra predstavke podnete od pojedinaca ili ponekad država. Presude su obavezujuće: država na koju se presuda odnosi je u obavezi da deluje u skladu sa njom i o tome se stara Komitet ministara koji, ako je potrebno, vrši politički pritisak na državu da izvrši odluku suda. Osim presuda, sud iznosi i savetodavna mišljenja.

[5] Direktiva, kao sekundarni izvor prava EU, po pravilu ne stvara neposredno prava i obaveze za fizička i pravna lica, već su njihovi adresati države članice. Dakle,

godine. Njoj je prethodila Konvencija o zaštiti lica u odnosu na automatsku obradu podataka iz 1985. godine. Predlagač konvencije je imao nameru da zemlje potpisnice usklade svoja nacionalna zakonodavstva sa osnovnim načelima i preporukama sadržanim u tom dokumentu. Budući da je do početka 1990. godine svega šest od 12 država članica (tadašnje) EEZ iskazalo saglasnost na obaveznost konvencijom, Evropska komisija je pristupila izradi Direktive 95/46 sa namerom da ujednači nivo zaštite prava na privatnost u EEZ (Poglavlje 3).

Direktiva 95/46 izražava težnju da se ostvare dva osnovna cilja: 1) zaštita osnovnih ljudskih prava i sloboda, i to naročito zaštita prava na privatnost u kontekstu obrade ličnih podataka, i 2) slobodan promet podataka o ličnosti između država članica EU (čl. 1).

Direktiva 95/46 se primenjuje na svaku obradu ličnih podataka, a ne samo na automatizovanu (čl. 3).

Ključne kategorije lica čija su prava i obaveze uređene Direktivom 95/46 jesu lica čiji se podaci obrađuju[6] i nadzornici.[7] Osnovna prava lica čiji se podaci obrađuju su pravo na obaveštenost, pravo na pristup prikupljenim podacima i pravo na protest.

U vezi sa pravom na obaveštenost lica čiji se podaci obrađuju izdvajamo članove 10 i 11 Direktive 95/46. U Direktivi 95/46 razlikuju se dve situacije: kada se podaci prikupljeni neposredno od lica čiji se podaci obrađuju (član 10) i kada su ti podaci prikupljeni posrednim putem (čl. 11). Direktivom 95/46 se proširuju obaveze obrađivača podataka, obavezujući ga da subjektu od koga bi da prikupi podatke već prilikom prikupljanja informacija pruži bitne informacije o

direktiva obavezuje države članice da donesu propise kojima će ostvariti ciljeve sadržane u datoj direktivi. Postupak donošenja direktive naziva se njenom transpozicijom. Kako je rok za transpoziciju Direktive 95/46 istekao krajem oktobra 1998. godine, sve države članice EU su usvojile odgovarajuće propise kojima ostvaruju ciljeve utvrđene u toj direktivi.

[6] Prema Directive 95/46/EC on the protection of persons in connection with the processing of personal data OJ L 281 of 23/11/1995, Art 2 (a), *lice čiji se podaci obrađuju* jeste svako lice čiji je identitet određen ili se može odrediti. Smatraće se da se identitet lica može odrediti kad kod je to na osnovu nekog podatka neposredno ili posredno moguće, a naročito kada se navode matični ili neki drugi identifikacioni broj nekog lica, odnosno jedan ili više elemenata karakterističnih za fizički, fiziološki, mentalni, ekonomski, društveni ili kulturni identitet tog lica.

[7] Prema Directive 95/46/EC on the protection of persons in connection with the processing of personal data OJ L 281 of 23/11/1995, Art 2 (d), *nadzornik* je fizičko ili pravno lice, organ javne vlasti, agencija ili drugo telo koje samostalno ili zajedno sa drugima utvrđuje svrhu i način obrade podataka o ličnosti.

cilju, obaveznosti ili dobrovoljnosti davanja podataka, o posledicama koje će ga pogoditi za slučaj da ne dâ podatke, kao i da ga obavesti o važnim pitanjima za njega i u slučaju da je podatke o njemu prikupio od trećeg lica.

Osim prava na obaveštenost, lica čiji se podaci obrađuju imaju i pravo na pristup tim podacima, što možemo primetiti u članu 12 Direktive 95/46. Države članice jemče svakom licu koje je predmet podataka pravo da, bez ograničenja u razumnim intervalima i bez prekomernog odgađanja ili troškova, od nadzornika dobije pre svega potvrdu o tome da li se podaci koji se na njega odnose obrađuju i obaveštenje barem o nameni obrade, kategoriji podataka o kojima je reč, o primaocima ili kategorijama primalaca kojima se ti podaci obelodanjuju, zatim da se to lice u razumljivom obliku obavesti o podacima koji se obrađuju, da mu se dostave sve raspoložive informacije o njihovom izvoru i da razume logiku na kojoj počiva svaka automatska obrada podataka koji se na njega odnose.[8]

Osim toga, pravo na pristup podacima podrazumeva i pravo lica čiji se podaci obrađuju da zatraži ispravke, brisanje ili blokiranje podataka čija obrada nije obavljena u skladu sa odredbama Direktive 95/46, posebno zbog nepotpune ili netačne prirode podatka, kao i da treće strane kojima su podaci bili obelodanjeni budu obaveštene o svakoj ispravci, brisanju ili blokiranju, sem ukoliko se pokaže da to nije moguće ili podrazumeva nesrazmeran napor.[9]

U vezi sa pravom lica čiji se podaci obrađuju da se suprotstavi obradi izdvajamo član 14 Direktive 95/46. Lice čiji se podaci obrađuju može da se, iz posebnih ličnih razloga, suprotstavi onoj obradi podataka o njemu koja je inače dopuštena i nadzornik tada podatke mora da obriše, osim ako obradom izvršava zakonsku obavezu. Da bi prava lica čiji se podaci obrađuju na odgovarajući način bila zaštićena, u Direktivi 95/46 je utvrđen čitav niz principa koji moraju biti primenjeni u postupcima prikupljanja i obrade podataka o ličnosti, koji su sadržani u članu šest Direktive 95/46 (Popović, Jovanović 2017, 134). Osnovni pricip u vezi sa prikupljanjem podataka jeste da se podaci o ličnosti smeju prikupljati u tačno određene, jasne i legitimne svrhe.

[8] Vid. Directive 95/46/EC on the protection of persons in connection with the processing of personal data OJ L 281 of 23/11/1995, Art 12 (a).

[9] Vid. Directive 95/46/EC on the protection of persons in connection with the processing of personal data OJ L 281 of 23/11/1995, Art 12 (b) i (c).

Direktiva 95/46 je značajna i zbog toga što uvodi presumpciju krivice obrađivača podataka u pogledu štete koja je prouzrokovana obradom (čl. 24), obavezuje države članice da uvedu nezavisan kontrolni organ koji se stara o primeni prava zaštite podataka o ličnosti (čl. 28–30), potpuno uređuje prekogranični prenos, to jest prenos podataka u zemlje koje nisu članice EU (čl. 25 i 26), čime se sada bavi i Dodatni protokol uz Konvenciju Saveta Evrope 108 (čl. 2).

3.3. Povelja EU o osnovnim pravima

Povelju EU o osnovnim pravima su 7. decembra 2000. godine svečano proglasili čelnici Evropskog parlamenta, Saveta EU i Evropske komisije. Povelja EU o osnovnim pravima je definitivno i u celini stekla pravnu obaveznost stupanjem na snagu Lisabonskog sporazuma 1. decembra 2009. godine (Popović, Jovanović 2017, 129).

Poveljom EU o osnovnim pravima garantuje se da svako ima pravo na zaštitu ličnih podataka u svim aspektima života: kod kuće, na poslu, prilikom kupovine, na lečenju, u policijskoj stanici ili na internetu (Baltezarević 2017, 246). Za pitanje zaštite ličnih podataka i privatnosti na internetu značajna je i odredba člana 8. Povelje EU o osnovnim pravima. Ta odredba nosi naziv „Zaštita podataka o ličnosti" i prema njoj svako ima pravo na zaštitu podataka o svojoj ličnosti (st. 1). Takođe, takvi podaci moraju biti obrađeni pošteno za unapred određenu svrhu i na osnovu informisanog pristanka osobe ili na nekom drugom legitimnom osnovu uređenom zakonom i svako ima pravo da pristupi prikupljenim podacima o svojoj ličnosti i pravo da zatraži njihovu ispravku (st. 2), a postupanje po tim pravilima je pod kontrolom nezavisnog organa (st. 3)

Tom odredbom se na opšti način uređuje pitanje zaštite ličnih podataka nezavisno od oblika u kome su sadržani i medijuma na kome su pohranjeni.

Osim u Povelji EU o osnovnim pravima, opšte odredbe o zaštiti podataka i privatnosti nalaze se i u Ugovoru o funkcionisanju Evropske unije (UFEU). Odredbom člana 16 Ugovora takođe je zajemčeno opšte pravo na zaštitu ličnih podataka. Prema toj odredbi, Evropski parlament i Veće utvrđuju pravila o zaštiti pojedinaca s obzirom na obradu ličnih podataka u institucijama, telima, uredima i agencijama EU, kao i u državama članicama kada obavljaju svoje aktivnosti u

području primene prava EU, a poštovanje tih pravila podleže nadzoru nezavisnih tela (st. 2).

Dakle, osnovna razlika između člana 16 UFEU i člana 8 Povelje EU o osnovnim pravima je ta što UFEU obavezuje Evropski parlament i Veće da, u skladu sa redovnim zakonodavnim postupkom, usvoje pravila kojima će se uređivati postupanje sa podacima o ličnosti i njihova obrada, a koja će obavezivati institucije, tela, službe i agencije EU, ali i države članice kada sprovode delatnosti i radnje u stvarima koje su uređene pravom EU.

3.4. Direktiva 2002/58

S obzirom na to da su nove napredne digitalne tehnologije zavladale mrežama javne komunikacije u društvu, pojavile su se posebne potrebe zaštite ličnih podataka i privatnosti korisnika. EU je 2002. godine usvojila novu regulativu – Direktivu o privatnosti i elektronskim komunikacijama (Direktiva 2002/58), (Milić 2019, *https://www.milic.rs/internet-pravo/ direktiva-o-privatnosti-i-elektronskim-komunikacijama-epd-i-uredba-o-e-privatnosti-epr/*).

Pre Direktive 2002/58, neka pitanja zaštite podataka o ličnosti u sektoru telekomunikacija bila su uređena Direktivom o obradi podataka o ličnosti i zaštiti privatnosti u sektoru telekomunikacija. Međutim, ubrzan razvoj tehnologije je već u prvim godinama 21. veka učinio jasnim da tu direktivu treba osavremeniti, a privatnosti u sektoru elektronskih komunikacija pružiti sveobuhvatniji sistem zaštite, pa je tako stupanjem na snagu Direktive 2002/58 Direktiva o obradi podataka o ličnosti i zaštiti privatnosti u sektoru telekomunikacija prestala da važi.

Cilj Direktive 2002/58 je, kako stoji u njenom članu 1, da dopuni Direktivu 95/46 i doprinese uspostavljanju jednakog nivoa zaštite osnovnih prava i sloboda, a pre svega prava na privatnost u obradi podataka o ličnosti u sektoru elektronskih komunikacija, i da obezbedi slobodu kretanja tih podataka i opreme za elektronsku komunikaciju u okviru EU. Direktiva 2002/58 je 2009. godine pretrpela značajne izmene i dopune (Popović, Jovanović 2017, 140).

Direktivom 2002/58 uređena su brojna važna pitanja zaštite podataka o ličnosti u kontekstu elektronskih komunikacija, kao što su bezbednost i poverljivost komunikacija, tretman podataka o saobraća-

ju poruka, spam (masovno slanje neželjenih poruka bez ikakvog kriterijuma) i tzv. kolačići.[10]

Suština obaveze pružanja bezbednosti je u tome da se obezbedi da podacima koji su predmet zaštite Direktive 2002/58 mogu da pristupe samo ovlašćena lica i da se spreči slučajno uništenje tih podataka. Pretnje po bezbednost podataka i komunikacije su tzv. špijunski programi, mrežne greške, skriveni identifikatori i druga slična sredstva koja mogu ući u korisnikov računar bez njegovog znanja, sa ciljem dobijanja pristupa informacijama, ubacivanja skrivenih informacija ili ulaženja u trag aktivnostima korisnika, čime mogu ozbiljno narušiti njegovu privatnost. Takva sredstva treba da budu dozvoljena isključivo u legitimne svrhe ili uz izričitu saglasnost korisnika. Jedno od tih sredstava su i tzv. kolačići (eng. *cookies*). Rani nacrti Direktive 2002/58 su predviđali potpunu zabranu korišćenja „kolačića" bez saglasnosti korisnika. Međutim, kako bi takav pristup imao negativne posledice na tehnološkom planu, postalo je jasno da se uređenju tretmana „kolačića" mora pristupiti na drugačiji način. U svojoj verziji iz 2002. godine Direktivom 2002/58 je bio predviđen tzv. *opt-out* pristup: države članice EU su bile dužne da obezbede da upotreba mreža za elektronsku komunikaciju u svrhu skladištenja informacija ili pristupa informacijama skladištenim u opremi pretplatnika ili korisnika bude dozvoljena samo pod uslovom da je pretplatnik ili korisnik na jasan i razumljiv način obavešten o svrsi obrade „kolačića" i da mu je bilo omogućeno da odbije tu ponudu. Prilikom izmena i dopuna Direktive 2009. godine ta odredba je promenjena i Direktiva sada prihvata tzv. *opt-in* pristup: obrada „kolačića" je dozvoljena ako je pretplatnik ili korisnik, pošto je na jasan i razumljiv način obavešten o svrsi obrade, dao svoju saglasnost za tu obradu.

U pogledu poverljivosti komunikacija,[11] Direktiva 2002/58 nalaže državama članicama da pravno onemoguće slušanje, prisluški-

[10] „Kolačići" su obično kratki kodirani zapisi koje generiše posećeni veb-sajt i koji ostaju zapamćeni u veb-pretraživaču korisničkog računara. Oni imaju nekoliko važnih uloga. Prva je da olakšaju upravljanje sesijom pretraživanja i korišćenja interneta. Primera radi, pomoću „kolačića" veb-sajtovi kao što je *YouTube* generišu predloge video-zapisa sličnih onim koje je korisnik ranije pregledao. Sa ovim je povezana i uloga „kolačića" u personalizaciji korišćenja interneta. Karakterističan primer je aktiviranje zapamćenih lozinki za pristup određenim sajtovima ili elektronskim bazama podataka pomoću „kolačića". Konačno, „kolačići" služe i za praćenje kretanja korisnika po svetskoj mreži, iz čega se mogu izvesti zaključci o njegovim interesovanjima, ukusu, navikama...

[11] Vid. Directive 2002/58/EC on privacy and electronic communications, OJ L 201 of 31/7/2002, Art 5.

vanje, skladištenje informacija o komunikacijama i bilo koji drugi vid presretanja ili nadzora elektronskih komunikacija bez saglasnosti korisnika na koje se ti podaci odnose. Zabrana nadzora i presretanja elektronskih komunikacija neće se primenjivati onda kada je to zakonom dozvoljeno, i to na način predviđen članom 15(1).

Tretman podataka o saobraćaju uređen je članom 6 Direktive 2002/58. Osnovna obaveza u tom pogledu jeste brisanje ili anonimizovanje podataka o saobraćaju koji se tiču pretplatnika ili korisnika čim dalje zadržavanje tih podataka postane nepotrebno za prenos komunikacije. Obaveza brisanja ili anonimizovanja podataka može biti izmenjena, odnosno ukinuta, pod uslovima predviđenim članom 15 (1) Direktive.

3.5. Direktiva 2016/680

Direktiva 2016/680 o zaštiti fizičkih lica u odnosu na obradu podataka od nadležnih organa u svrhe sprečavanja, istrage, otkrivanja ili vođenja postupaka za krivična dela, odnosno izvršenja krivičnih sankcija, i o slobodnom prometu takvih podataka usvojena je istovremeno sa Uredbom 2016/679. Počela je da se primenjuje 5. maja 2016. godine.

U Direktivi 2016/680 je izraženo nastojanje da se „preslikaju" osnovni principi utemeljeni Direktivom 95/46 i Uredbom 2016/679. Zato ne iznenađuje to što su opšta arhitektura Direktive 2016/680, a naročito prava lica čiji se podaci obrađuju i dužnosti nadzornika, u velikoj meri podudarni onima koji su predviđeni Direktivom 95/46, odnosno Uredbom 2016/679.[12]

Direktivom 2016/680 se štite pojedinci kada vlasti obrađuju njihove lične podatke u svrhu prevencije, istrage, otkrivanja ili gonjenja krivičnih dela ili za izvršavanje krivičnih kazni. Prema toj direktivi, svačiji lični podaci moraju da se obrađuju zakonito, pošteno i samo za određenu svrhu, koja je uvek povezana sa borbom protiv kriminala. Direktivom 2016/680 se osigurava da obrada ličnih podataka širom EU bude u skladu sa principima zakonitosti, proporcionalnosti i neophodnosti, uz odgovarajuće mere zaštite pojedinca. Takođe, njome se nacionalnim organima za zaštitu podataka obezbeđuje potpuno nezavisan nadzor.

[12] Baš kao i Uredba 2016/679, i Direktiva 95/46 u krivičnim stvarima predviđa postojanje oficira za zaštitu podataka, uvođenje nadzornog tela.

Iako je Direktiva 2016/680 izraz nastojanja da se prava država članica EU harmonizuju u širokom krugu pitanja zaštite podataka o ličnosti prikupljenih ili obrađenih u okviru policijske i pravosudne saradnje, u određenim aspektima se državama članicama ostavlja sloboda da pojedina pitanja urede na način koji je najprikladniji za pravnu tradiciju svake države pojedinačno (npr. čl. 56 i 57).

3.6. Uredba 2016/679

U EU je u maju 2018. godine na snagu stupila Opšta uredba o zaštiti podataka (Uredba 2016/679), kao finale dugogodišnjeg procesa. Usaglašavanje konačne verzije teksta trajalo je četiri godine (2012–2016), na sam tekst je podneto rekordnih 4000 amandmana, dok su u javnoj raspravi učestvovali gotovo svi relevantni akteri iz javnog, privatnog i civilnog sektora.

Iako se Uredba 2016/679 predstavlja kao svojevrsna revolucija koja iz korena menja pravila zaštite podataka, nova regulativa je ipak prirodni naslednik Direktive 95/46 i suštinski se nadovezuje na iste principe i norme. Regulatori su iskoristili priliku da dodatno urede brojna sporna pitanja nastala tokom razvoja interneta i novih tehnologija (Krivokapić *et al*. 2019, 13). Tako se, na primer, Uredbom 2016/679 uvode pojmovi povrede podataka o ličnosti, pseudonimizacije, biometrijskih podataka i, između ostalog, definiše pojam glavnog mesta poslovnog nastanjenja, što je veoma važno za primenu pravila o kontroli i ograničenjima slobode prikupljanja i obrade podataka.

Uredbom 2016/679 se uvodi i jedna nova kategorija subjekata. To je oficir za zaštitu podataka – lice zaduženo da obaveštava i savetuje nadzornika ili obrađivača, odnosno zaposlene na obradi podataka, o obavezama koje proizilaze iz Uredbe 2016/679 ili nacionalnih propisa država članica o zaštiti podataka i da sarađuje sa nadzornim telima. U članu 37 Uredbe 2016/679 navodi se da je imenovanje oficira za zaštitu podataka obavezno kada podatke o ličnosti obrađuje javno telo (izuzev sudova, ali samo u sklopu obavljanja pravosudne funkcije), kada se suština aktivnosti nadzornika ili obrađivača sastoji od radnji obrade podataka koje zahtevaju stalan i sistematski nadzor velikog broja lica čiji se podaci obrađuju i kada se u velikom broju obrađuju posebno osetljive kategorije podataka i podaci koji se odnose na krivičnu osuđivanost (Popović, Jovanović 2017, 137).

Uredbom 2016/679, u odnosu na Direktivu 95/46, znatno se proširuju prava lica čiji se podaci obrađuju. Uredba 2016/679 sadrži pravo da se ograniči obrada podataka (čl. 18), pravo na prenosivost podataka (čl. 20) ili pravo protesta čak i u slučaju obrade podataka u naučne, istorijske ili statističke svrhe (čl. 21 st. 6 i čl. 83 st. 1). Iako se Uredba 2016/679 direktno primenjuje u svih 28 članica, EU i dalje ostavlja prostor državama članicama da mnoge detalje samostalno regulišu u skladu sa svojim nacionalnim propisima. Takođe, Uredba 2016/679 štiti prava građana EU, što znači da se njene odredbe odnose na svaku organizaciju u svetu koja obrađuje podatke stanovnika zemalja članica EU, bilo da im nudi robu i usluge ili prati njihovo ponašanje na internetu (Krivokapić *et al*. 2019, 15).

4. ZAKLJUČAK

Globalizacija, kao metod širenja i rasprostiranja svega što društvo prihvata i usvaja kao adekvatno za dalji rast i sve ono što ima potencijal da pomogne i unapredi trenutno stanje u kojem se nalazimo, najzaslužnija je i za neverovatan razvoj i primenu tehnologije na svim poljima koje čovek može da zamisli (Milovanović 2019). Nova informaciona tehnologija našla je široku primenu u mnogim oblastima života i rada. Izvorno nastale da bi se komunikacija među ljudima na internetu učinila jednostavnijom i bržom, te tehnologije su postale i predmet raznih zloupotreba, te ih vešti pojedinci danas koriste suprotno njihovoj osnovnoj nameni, da bi za sebe ili drugoga izvukli nekakvu korist (Šarkić *et al*. 2007,121).

Razvojem interneta otvoren je čitav niz pitanja, a pre svega pitanje zaštite prava građana na privatnost, odnosno prava na nepovredivost integriteta njegove ličnosti (Lilić 2006, 140). To je imalo za posledicu da „pravo na privatnost" počne da se posmatra kao jedno od osnovnih ljudskih prava.

Problematika privatnosti je postala jedna od najvažnijih tema u uslovima upotrebe informaciono-komunikacionih tehnologija. Opasnost od tehnologije postaje veća jer, sa gledišta sigurnosti, internet ima velike slabosti. Istovremeno, u virtuelnom svetu čovek je daleko manje oprezan nego u realnom. Prividna nevidljivost i udaljenost stvaraju osećaj anonimnosti i sigurnosti, pa korisnik često ostavlja lične

podatke ili preduzima radnje kojima nesvesno ugrožava svoju bezbednost (Dimitrijević 2011, 244).

Postojanje opasnosti i rizika ukazalo je na neophodnost formiranja jednog sistema načela i mera za zaštitu prava na privatnost i tajnost podataka koji se na nju odnose. Takav jedan sistem su pokušale da uspostave države članice EU (Bosnić 1998, 26).

U donetim pravnim regulativama države članice EU su utvrdile osnovne ciljeve, principe i načela zaštite podataka o ličnosti, kriterijume kvaliteta i legitimnosti obrade podataka o ličnosti, posebne kategorije podataka, prava lica o kojima se podaci vode na pristup podacima, izuzeća i ograničenja tih prava kao i mere za zaštitu lica na koja se podaci odnose (Bosnić 1998, 28).

Međutim, teško je sa sigurnošću tvrditi koliko će akti EU o zaštiti podataka o ličnosti pozitivno uticati na poslovne aktivnosti i pravne odnose. Već se pojavljuju mišljenja stručne javnosti da su pojedini akti EU nepotpuni i da njima nisu obuhvaćene pojedine oblasti novih tehnologija. Nažalost, praksa EU i svih ostalih država pokazuje da pravo sporo reaguje kada je razvoj tehnologije u pitanju i da je na sceni društveni paradoks: nove tehnologije se stalno menjaju i unapređuju, a pravo te promene sporo prepoznaje (Baltezarević 2017, 249).

LITERATURA

1. Acquist, Alessandro, Ralph Gross. 6/2006. Imagined communities: awareness, information sharing, and privacy on the Facebook. *Privacy Enhancing Technologies*. Cambridge, UK Volume: LNCS, 4258: 36–58
2. Baltezarević, Vesna, Radoslav Baltezarević. 1/2017. Zaštita privatnosti na internetu – evropski model. *Megatrend revija* 14: 241–252.
3. Baltezarević, Vesna, Radoslav Baltezarević. 7/2015. Sloboda na internetu i njene posledice. *Godišnjak Fakulteta za kulturu i medije*: 257–272.
4. Bosnić, Jadranka. 1–2/1998. Zaštita podataka o ličnosti. *Jugoslovenski časopis za pravnu informatiku* 6: 26–35.
5. Dimitrijević, Predrag. 2011. *Pravo informacione tehnologije*. Niš: Centar za publikacije Pravnog fakulteta u Nišu.
6. Kol, Erik. 2021. *Onlajn opasnost*. Beograd: Vulkan izdavaštvo.
7. Krivokapić, Danilo, Jelena Adamović, Dunja Tasić, Andrej Petrovski, Petar Kalezić, Đorđe Krivokapić. 3/2019. Novo doba zaštite podataka o ličnosti. *Prelom* 61: 13–15.

8. Lilić, Stevan. 2006. *Pravna informatika*. Beograd: Zavod za udžbenike i nastavna sredstva.
9. Milovanović, Sandra. 2019. *Nasilje na internetu – kriminološki aspekt*. Neobjavljeni rukopis. Niš: Pravni fakultet Univerziteta u Nišu.
10. Popović, Miloš. 2016. *Internet i mladi.* Neobjavljeni rukopis. Niš: Pravni fakultet Univerziteta u Nišu.
11. Popović, Dušan, Marko Jovanović. 2017. *Pravo interneta*. Beograd: Centar za izdavaštvo i informisanje.
12. Šarkić, Nebojša, Dragan Prlja, Katarina Damnjanović, Vesna Živković, Vladimir Marić, Vladimir V. Vodinelić, Nataša Mrvić Petrović. 2007. *Pravo informacionih tehnologija*. Beograd: Pravni fakultet Univerziteta Union u Beogradu – Javno preduzeće „Službeni glasnik".
13. Kuzmanović, Dobrinka. 2019. Zaštita ličnih podataka i privatnost na internetu. *https://digitalni-vodic.ucpd.rs/zastita-licnih-podataka-i-privatnosti-na-internetu/?lng=lat*, poslednji pristup 20. jula 2023.
14. Khandelwai, Swati. 2017. Sweden Accidentally Leaks Personal Details of Nearly All Citizens. *https://thehackernews.com/2017/07/sweden-data-breach.html*, poslednji pristup 23. jula 2023.
15. Milić, Dragan. 2019. Direktiva o privatnosti i elektronskim komunikacijama (ePD) i Uredba o e-privatnosti (ePD). *https://www.milic.rs/internet-pravo/direktiva-o-privatnosti-i-elektronskim-komunikacijama-epd-i-uredba-o-e-privatnosti-epr/*, poslednji pristup 10. avgusta 2023.

Marija Vojisavljević*

EUROPEAN REGULATION OF DATA PROTECTION ON THE INTERNET

Summary: The right to privacy is particularly threatened by the emergence of new information technologies. In a time characterized by the processing of huge amounts of various data, the so-called "era of big data", personal data is treated as the most important resource. The Internet has made it possible to access data that can be misused. Recognizing the dangers that the Internet brings with it, the members of the European Union have undertaken a number of important activities with the aim of protecting the rights of Internet u1sers and providing them with security on the networks. This paper presents the provisions and principles of protection of personal data and privacy on the Internet contained in the European Convention for the Protection of Human Rights and Fundamental Freedoms, Directive 95/46, the Charter of the European Union on Fundamental Rights, Directive 2002/58, Directive 2016/680 and General regulation on data protection. Conventions, regulations and directives are reviewed to determine to what extent the European Union has succeeded in its intention to find adequate legal regulation of data protection on the Internet.

Key words: *Internet, Legal Acts of the European Union, Online threats, Personal data, Privacy*

* Author is an undergraduate student at the University of Belgrade – Faculty of Law, *marijavojisavljevic2003@gmail.com*.

UDK 343.525:004.738.5
DOI 10.51204/IVRS_24106A

Nataša Ranković*

KRAĐA IDENTITETA KAO KRIVIČNO DELO: *DE LEGE LATA* I *DE LEGE FERENDA*

U radu su definisani osnovni pojavni oblici kompjuterskog kriminala sa akcentom na krađu identiteta kao posebnom obliku koji bi de lege ferenda okarakterisali i adekvatno propisali kao krivično delo u Krivičnom zakponiku Republike Srbije. Cilj ovog rada je da se pokaže mesto krađe identiteta u spektru raznih kriminalnih radnji koje se svrstavaju u visokotehnološki kriminal. Rad je podeljen na tri celine. Prva predstavlja uvodno izlaganje u kome je opisan način na koji utiče veoma brz razvoj informacionih i komunikacionih tehnologija na razvijanje novih metoda za njihovu zloupotrebu, nakon čega su opisane definicije krađe identiteta i njene karakteristike. Drugi deo rada je posvećen načinima, obeležjima i modalitetima krađe identiteta, dok je u trećem delu značaj dat načinima zaštite i prevencije krađe identiteta te argumentovan predlog za njeno definisanje u Krivičnom zakoniku Republike Srbije. Na kraju rada dat je kratak sažetak u vidu zaključka.

Ključne reči: *visokotehnološki kriminal, kompjuterski kriminal, krađa identiteta, krivični zakonik, krivično delo*

1. UVOD

Napretkom i brzinom razvoja informacionih i komunikacionih tehnologija recipročno raste broj njihove zloupotrebe u vidu narušavanja poverljivosti informacija, ometanja njihove funkcionalnosti, uzurpiranja i krađe intelektualnih dobara i raznih vrsta krađa i prevara. Visokotehnološki kriminal je relativno nov oblik kriminalnog ponašanja, veoma složen i adaptivan u odnosu na brzinu razvoja tehnologije, lako se širi i razvija nove oblike. Prilikom određivanja termina visokotehnološkog kriminala može se naići na veliki broj različitih definicija, međutim svima je zajednički element vršenje kriminalne radnje kori-

* Autorka je studentkinja osnovnih akademskih studija na Pravnom fakultetu Univerziteta u Beogradu, *natasarankovic24@gmail.com*.

šćenjem tehnika visoke tehnologije, pri čemu je naneta šteta žrtvama kriminalne radnje.

Mrežno okruženje i internet pružaju širok dijapazon mogućnosti za krađu i poslovnih i drugih tajni, softvera i autorskih dela, ali predstavljaju i veoma pogodno područje za krađu ličnih tajni i njihovu zloupotrebu krađom novca i drugim napadima na ličnost. Krađa identiteta kao oblik visokotehnološkog kriminala prolazila je kroz razne faze definisanja, međutim svi bitni elementi obuhvaćeni su sledećim određivanjem: „Krađa identiteta je forma kriminala u kojem neko koristi tuđi identitet da bi izvršio kriminalnu radnju" (Đukić 2017, 100). Krađa identiteta je zapravo poseban oblik visokotehnološkog kriminala koji objedinjuje nelegalno pribavljanje poverljivih ličih podataka za jedno ili više lica i upotrebu tih podataka za izvršenje novih krivičnih dela, pri čemu se nelegalno pribavljanje podataka o ličnosti obavlja bez znanja osobe koja predstavlja žrtvu uz prisvajanje njenog imena i drugih ličnih podataka. Kako smo videli, jedan od uočljivijih fenomena savremenog sveta je sve češće korišćenje podataka nekog drugog lica sa ciljem da se pribavi nekakva korist ili da se nanese šteta. Iz tog razloga se pribegava različitim propisima kojima se definišu jasna pravila o postupanju sa podacima o ličnosti, uređuje se kako se s njima postupa, kako se čuvaju i po potrebi uništavaju. U svetlu toga nezaobilazno je pitanje – kako stvari stoje kod nas?

2. POJAM KRAĐE IDENTITETA

Krivična dela koja spadaju u visokotehnološki kriminal uslovno se mogu podeliti na dve vrste – krivična dela koja se tiču isključivo visokotehnološkog kriminala i krivična dela koja imaju elemente visokotehnološkog kriminala, ali nisu isključivo u nadležnosti Posebnog tužilaštva i Odeljenja za suzbijanje visokotehnološkog kriminala. Prvu grupu krivičnih dela čine krivična dela koja su uređena u glavi dvadeset sedam Krivičnog zakonika[1] (čl. 298–304a). U drugu grupu spada mnogo više krivičnih dela nego u prvu. To su krivična dela protiv intelektualne svojine (član 198, 199, 202), ali i pojedinačna krivična dela, kao što su ugrožavanje sigurnosti, najčešće putem društvenih mreža (čl. 138), neovlašćeno objavljivanje i prikazivanje tuđeg spisa, portreta

[1] Krivični zakonik Srbije – KZ, *Sl. glasnik RS* 85/2005, 88/2005 – ispr., 107/2005 – ispr., 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 i 35/2019.

i snimka (čl. 145), neovlašćeno prikupljanje ličnih podataka (čl. 146), prikazivanje, pribavljanje i posedovanje pornografskog materijala i iskorišćavanje maloletnog lica za pornografiju (čl. 185), iskorišćavanje računarske mreže ili komunikacije drugim tehničkim sredstvima za izvršenje krivičnog dela protiv polne slobode prema maloletnom licu (čl. 185b), falsifikovanje i zloupotreba platnih kartica (čl. 243) i druga krivična dela za čije se izvršenje koriste računari.

Izraz „socijalni inženjering" se često u istoriji spominjao kao zamena za izraz „krađa identiteta". Socijalni inženjering, u značenju u kojem je ranije korišćen, podrazumevao je širok dijapazon načina manipulisanja ljudima ubeđivanjem i lažnim predstavljanjem radi pribavljanja željenih informacija, pri čemu se nisu morala koristiti tehnička sredstva. Dakle, socijalni inženjering je u sadržajnom smislu širi pojam od krađe identiteta. Pod opštim pojmom krađe identiteta mogu se podrazumevati različiti modeli i pojavni oblici krađe podataka o ličnosti i veliki broj metoda i postupaka njihove upotrebe prilikom izvršenja novih kriminalnih radnji (Đukić 2017, 101).

Pojavom interneta, računari su počeli da se koriste za krađu informacija, novca i mnogih drugih stvari, međutim, neretko se dešava da lopovi kradu celokupan identitet strpljivo, prikupljajući informacije i podatke nekog lica. Sve većim i bržim razvojem novih tehnologija značajno se olakšavaju prikupljanje ličnih informacija, njihovo deljenje, ali i njihova zloupotreba. Zanimljivo je to što polaznu tačku za izvršenje kriminalnih dela čine različite vrste drugih oblika kriminalnih aktivnosti koje se dovode u vezu sa sajber kriminalom i koje u osnovi, zapravo, imaju krađu identiteta (Vidojković 2015, 47).

Dragan Prlja i Mario Reljanović su se bavili određivanjem pojma krađe identiteta. U svom radu govore o krađi lika i identiteta i drugim vidovima (ne)zakonitog ponašanja, a krađu identiteta određuju kao: „preuzimanje 'uloge' nekog lica na Internetu, redovno u cilju sticanja neke materijalne ili druge koristi" (Prlja, Reljanović 169). Prlja i Reljanović karakterizuju krađu identiteta kao: najdrastičniji atak na privatnost ličnosti jer se učinilac, nakon što je prevarom ili na drugi način došao do vitalnih podataka za preuzimanje nečijeg identiteta (internet i druge šifre, brojevi platnih kartica i sl.), predstavlja u njegovo ime, zaključuje poslove ili ostvaruje društvene kontakte, ispravno primećujući i da može vršiti krivična dela na taj način, prikriven iza tuđeg identiteta (Prlja, Ivanović, Reljanović 2011, 110). U svom radu su pružili i sopstvenu definiciju po kojoj: krađa identiteta pretpostavlja prethodno

izvršenje nekog drugog krivičnog dela kao što su prevare, upadi u tuđi računar ili računarski sistem itd.

Krađa identiteta je krivično delo u čijem se izvršenju neko lice lažno predstavlja kao drugo lice (sa identifikacionim podacima tog drugog lica) sa namerom da pribavi protivpravnu imovinsku korist ili druge lične koristi. Žrtva ili pasivni subjekt tog dela može biti fizičko ali i pravno lice, kao što i izvršilac može biti pojedinac ili više lica, koja predstavljaju delove organizovane grupe (Prlja, Ivanović, Reljanović 2011, 108). Ne možemo reći da je redak slučaj da se krađa identiteta koristi kao sekundarno krivično delo kako bi se izvršilo primarno, gde se pojavljuje kao sredstvo kojim se vrši glavno delo, kako bi izvršilac sakrio svoj trag. Klasični primeri takvog načina izvršenja, danas svima poznati, jesu prevare sa kreditnim karticama i podnošenje lažnih dokumenata za dobijanje kredita na ime lica čiji je identitet ukraden.

Kao što možemo videti, u najvećem broju slučajeva krajnji cilj krađe identiteta je izvršenje novog krivičnog dela čija posledica može biti materijalne ili nematerijalne prirode. Iz tog razloga je u mnogim anglosaksonskim državama predviđena kao krivično delo, dok evrokontinentalne države stoje na stanovištu da je identitet na adekvatan način dovoljno zaštićen postojećim krivičnim delima poput prevare, lažnog predstavljanja, falsifikovanja isprave, neovlašćenog prikupljanja ličnih podataka i sl. (Bajović 2018, 262).

3. OBELEŽJA I MODALITETI KRAĐE IDENTITETA

Izraz „fišing" se u savremenoj literaturi definiše kao najčešći vid krađe identiteta koji podrazumeva skup aktivnosti kojima neovlašćena lica korišćenjem lažnih elektronski poruka ili lažnih internet stranica korisnike interneta navode da otkriju poverljive podatke (JMBG, korisničko ime, lozinku, PIN kartice i sl.).

Prevaranti metodom fišinga ili širenjem računarskih virusa preuzimaju lozinke i otimaju mejl adrese korisnika, a čitanjem mejlova dolaze do značajnih saznanja o toj osobi. Ako, recimo, saznaju da je neko otputovao u inostranstvo, ne libe se da sa njegove internet adrese, nakon što preuzmu kontrolu nad njom, poznanicima žrtve pošalju poruke. Lažno se predstave kao da su vlasnici tog naloga, tvrde da su pokradeni i da treba da im se na određeni račun uplati novac da bi doputovali kući (Ivanović 2021, 284).

Korisnici interneta imaju sve veću svest i znanje o fišingu te su oprezniji, ali su izvršioci takvih krivičnih dela u koraku sa razvojem tehnologije, pa su razvili nove tehnike. Slanje poruka kojima se korisnici ubeđuju da posete neku internet stranicu na adresi iz lažne poruke zamenili su virusima kako bi se od žrtava prevare preuzimali osetljivi podaci.

Zahvaljujući sve bržem razvoju tehnologije, razvijaju se i razne vrste fišinga: farming, spam, ciljani fišing, fišing pretraživačkih servisa, koji se, kao noviji oblik fišing prevare, sastoji u kreiranju veb-stranica (sajtova) u vezi s lažnim proizvodima i uz pomoć kojeg izvršilac dolazi do poverljivih informacija tako što žrtvu navede da naruči te lažne proizvode ili da se loguje na takve sajtove.[2]

S obzirom na karakteristike te vrste napada, može se reći da je fišing izrazito sofisticirana pojava, koja je u velikom usponu. Kao izvršioci se ne javljaju amateri već su najčešće u pitanju profesionalci, organizovani u grupe sa vrlo preciznim ulogama i delatnostima. Takođe, veoma je moguća veza tog oblika kriminala sa organizovanim kriminalom (Ivanović 2021, 294).

Krađe identiteta na osnovu pribavljenih informacija o ličnosti mogu se ostvariti na više načina: zloupotrebom postojećih računa (kreditnih kartica, tekućih bankovnih računa); zloupotrebom postojećih računa (na kojima nisu izdate kreditne i platne kartice) i zloupotrebom postojećih uz korišćenje debitnih i kreditnih kartica, a moguće je vršiti i klasična krivična dela, kao što su falsifikovanje kartice ili zloupotreba postojećih podataka (Ivanović 2021, 332).

Munjevitim napretkom tehnologije, internet servisi postaju pogodan ambijent za krađu i zloupotrebu identiteta. Krađa identiteta započinje prisvajanjem ličnih podataka o nekom licu, bez pristanka i znanja tog lica, obmanom, krađom i prevarom, a nastavlja se upotrebom prikupljenih podataka za izvršenje krivičnih dela koja se u najvećem broju slučajeva odnose na sticanje protivpravne imovinske koristi licima koja zloupotrebljavaju ukradeni identitet (Milošević, Urošević 2009, 53–64).

Ne može se reći da je redak slučaj da se krađa identiteta, korišćena kao sekundarno krivično delo kako bi se izvršilo primarno, pojavljuje i kao sredstvo kojim se vrši glavno delo, kako bi izvršilac sakrio svoj trag ili ga zametnuo (Marković 2021, 7). Klasični, svakome po-

[2] Više o tome u: Ivanović 2021, 288–300.

znati primeri su prevare sa kreditnim karticama ili podnošenje lažnih dokumenata za dobijanje kredita na ime lica čiji je identitet ukraden.

Krađe podataka se naširoko koriste u fišing napadima sa ciljem komercijalne i industrijske špijunaže, na osnovu pretpostavke da se na privatnim računarima zaposlenih nalaze veće količine poverljivih informacija i podataka o njihovih firmi. Tim putem se može doći i do dokumentacije kao što su poslovna prepiska ili dokumenti o zaštićenim dizajnima, čijim se objavljivanjem nanosi ekonomska šteta ili urušava reputacija žrtve (Ivanović 2021, 297). Dakle, u najvećem broju slučajeva krajnji cilj krađe identiteta je izvršenje novog krivičnog dela, čija posledica može biti materijalne ili nematerijalne prirode, zbog čega je u mnogim anglosaksonskim državama predviđena kao krivično delo, dok se evrokontinentalne države drže mišljenja da je identitet na adekvatan način i dovoljno zaštićen postojećim krivičnim delima (prevara, falsifikovanje, zloupotreba, lažno predstavljanje).

Krađa identiteta ima i međunarodnu dimenziju. Obično izvršioci i žrtve nisu u istim državama, što povlači pitanja jurisdikcija, primenu načela *nullum crimen nulla poena sine lege* i probleme nadležnosti institucija za saradnju (Ivanović 2021, 339).

4. ZAŠTITA I PREVENCIJA OD KRAĐE IDENTITETA

Zvonimir Ivanović zauzima pozitivan stav kada je reč o postojanju potrebe da se na adekvatan i sveobuhvatan način definiše krivično delo krađe identiteta. Međutim, kako se pojam krađe identiteta koristi veoma neprecizno, čemu doprinosi nepostojanje opšteprihvaćene definicije, inkriminacija krađe identiteta je otežana već na samom početku. Pojam krađe identiteta se prvenstveno koristi u značenju krađe, to jest radnje pribavljanja i upotrebe identifikacionih obeležja drugog lica, a s druge strane taj termin označava i krivična dela izvršena upotrebom tuđeg identiteta putem tuđih identifikacionih obeležja.

Velika Britanija krađu identiteta nije smatrala krivičnim delom sve do 2007. godine kada je prevara inkriminisana u zakonu *UK Fraud Act 2006*[3], obuhvatajući i prevaru izvršenu onlajn. Prema tom zakonu, prevara se može izvršiti na tri načina: 1. lažnim predstavljanjem, pri-

[3] Fraud Act 2006, Chapter 35. *https://www.legislation.gov.uk/ukpga/2006/35*, poslednji pristup 26. septembra 2023.

kazivanjem činjenica, 2. namernim neiznošenjem i prikrivanjem činjenica i 3. zloupotrebom položaja i odnosa podređenosti ili zavisnosti.

Možda najbolje inkriminisana krađa identiteta, kako tvrdi Ivanović (2021, 340), u SAD se definiše pod naslovom prevara i aktivnosti povezane sa identifikacionim dokumentima, autentifikacionim sredstvima i informacijama, te se pod krađom identiteta podrazumeva: „svesno transferisanje, posedovanje ili korišćenje, bez zakonskog ovlašćenja, sredstva za identifikaciju drugog lica u nameri izvršenja, pomaganja ili navođenja na izvršenje, ili u vezi sa delom, koje predstavlja delo kažnjivo delo po federalnom ili zakonu države članice SAD, kao i lokalnim propisima".[4] Tim delom se pokriva širok dijapazon radnji povezanih sa identifikacionim sredstvima, pa tako i krađom identiteta.

Kanada je krajem 2007. godine uvela krađu identiteta kao poseban oblik krivičnog dela, a kao razlog za preciznije definisanje navedena je okolnost da postojeći krivični zakon ne obuhvata sve elemente tog krivičnog dela. Naime, zloupotreba tuđeg identiteta je pokrivena zakonom kao falsifikovanje ili lažno predstavljanje, ali pripremne radnje za krađu identiteta, kao što su prikupljanje, posedovanje i promet podataka za identifikaciju, nisu obuhvaćene postojećim krivičnim delima. Svrha inkriminacije tih krivičnih dela je popunjavanje praznina u krivičnom zakonu (Ivanović 2021, 335).

Što se tiče standarda, Srbija je 2006. godine potpisala Konvenciju 108 Saveta Evrope, kojom se reguliše oblast zaštite podataka, čime je na sebe preuzela određeni standard u toj oblasti, ali ga, međutim, u praksi slabo primenjuje (Đalović 2018, 28). U navođenju zakona kojima se indirektno reguliše oblast računarske prevare, neophodno je naglasiti da krađa identiteta nije *de lege lata* inkriminisana kao krivično delo u krivičnom zakonodavstvu. Neki od zakona kojima se reguliše ta oblast su: Zakon o elektronskim komunikacijama, Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala, Zakon o zaštiti podataka o ličnosti i Zakon o potvrđivanju Konvencije o visokotehnološkom kriminalu.

Ivanović naglašava da je u određivanju prostora za inkriminaciju krađe identiteta neophodno prepoznati nekoliko segmenata samog akta koji bi se mogao definisati kao prevarno pribavljanje i korišće-

[4] United States Code (U.S.C.) Title 18, Section 1028 (a) (7): „a single identification document or false identification document that contains 1 or more means of identification shall be construed to be 1 means of identification".

nje identifikacionih obeležja drugog lica. Akcenat stavlja na to da se delo može izvršiti fizičkim putem, bez primene tehničkih i tehnoloških sredstava, ali i uz pomoć, u svakodnevnim životima sve zastupljenijih, interneta i tehničkih i tehnoloških metoda.

Takođe, izdvaja i tri faze napada: 1. izvršilac ubeđuje žrtvu, metodama socijalnog inženjeringa, da otkrije poverljive informacije i podatke na određenom sajtu u nameri da ih koristi u kriminalne svrhe; 2. izvršilac pribavlja podatke o kreditnim karticama ili debitnim karticama žrtve, koje potom koristi za naručivanje ili pribavljanje robe i usluga; 3. izvršilac pribavlja podatke o korisničkom imenu i lozinki na internet nalogu i imejl adresu i koristi ih da šalje mejlove sa negativnim sadržajem (Ivanović 2021, 338). Može se zaključiti da Ivanović, na osnovu izloženih zakonskih inkriminacija, smatra da, u smislu pokrivenosti i u odnosu na svakodnevno ažuriranje i menjanje pojavnih oblika, tradicionalnim oblicima krivičnih dela ne može da bude potpuno obuhvaćeno svako delo te vrste.

5. ZAKLJUČAK

Sve brži i sve turbulentniji napredak tehnologija znatno olakšava njihovo korišćenje, ali i zloupotrebu, pa se tako sve češće javljaju slučajevi kriminala putem interneta. Internet je, kako vidimo, pogodno tle za razne vrste kriminala, od povrede prava na privatnost zloupotrebom društvenih mreža, pa sve do krađe identiteta. Krađa identiteta je u domaćem krivičnom zakonodavstvu indirektno uređena drugim propisima (primera radi: neovlašćen pristup zaštićenom računaru, zloupotreba podataka o ličnosti i dr.), međutim, radi preciznijeg i bližeg određivanja i jednostavnijeg određivanja sankcija, krađa identiteta bi mogla da se podvede pod krivična dela visokotehnološkog kriminala, krivična dela protiv bezbednosti računarskih podataka, pomenuta krivična dela neovlašćen pristup zaštićenom računaru i zloupotreba podataka o ličnosti itd. Opet, tu se javlja problem pod koje krivično delo podvesti krađu identiteta tako da bude na adekvatan način definisana i sankcionisana, a da pri tome obuhvati sve oblike u kojima se javlja. Značajno je obratiti pažnju na to kako je krađa identiteta definisana u SAD jer je tim krivičnim delom obuhvaćen širok dijapazon radnji povezanih aa identifikacionim sredstvima, što smanjuje

mogućnost pojave praznina u njihovom krivičnom zakonodavstvu. To je dobar primer inkriminacije i jasnijeg određivanja i definisanja krađe identiteta koji bi mogao da bude koristan za eventualno preciziranje i definisanje krađe identiteta u domaćem krivičnom zakonodavstvu. Situacija u domaćem zakonodavstvu je najsličnija onoj u kanadskom, pa možemo povući paralelu u kontekstu analogije u odnosu na njega i u nekoj skorijoj budućnosti, vodeći se primerom inkriminacije krađe identiteta u kanadskom ili krivičnom zakonodavstvu SAD, u domaće uvesti krivično delo krađe identiteta.

LITERATURA

1. Antonović, Ratomir. 2023. *Sajber kriminalitet kao kriminalitet današnjice*. Beograd: Centar za stratešku analizu.
2. Bajović, Vanja. 2018. *Krađa identiteta i krivičnopravna zaštita ličnih podataka u sajber okruženju*. Beograd: Pravni fakultet Univerziteta u Beoradu.
3. Vidojković, Miloš. 2015. *Kompjuterski kriminalitet*. Master rad. Niš: Pravni fakultet Univerziteta u Nišu.
4. Đalović, Ratko. 2018. *Krađa identiteta*. Diplomski rad. Beograd: Fakultet bezbednosti Univerziteta u Beogradu.
5. Đukić, Anđelija. 2017. *Krađa identiteta – oblici, karakteristike i rasprostranjenost*. Beograd: Fakultet bezbednosti Univerziteta u Beogradu.
6. Ivanović, Zvonimir. 2021. *Kriminalistički aspekti visokotehnološkog kriminala*. Beograd: Kriminalističko-policijski univerzitet u Beogradu.
7. Marković, Stefan. 2021. *Mogućnost suprotstavljanja visokotehnološkom kriminalu u Republici Srbiji*. Master rad. Beograd: Fakultet bezbednosti Univerziteta u Beogradu.
8. Milošević, Milan. 1/2007. Aktuelni problemi suzbijanja kompjuterskog kriminala. *NBP (Nauka, bezbednost, policija)* 12: 57–74.
9. Milošević, Milan, Vladimir Urošević. 2009. Krađa identiteta zloupotrebom informacionih tehnologija. 53–64. *Bezbednost u postmodernom ambijentu*, zbornik radova, knjiga VI.
10. Mirković, Dragan. 2017. *Kriminološki aspekti komputerskog kriminaliteta*. Niš: Pravni fakultet Univerziteta u Nišu.
11. Prlja, Dragan, Mario Reljanović. 3/2009. Visokotehnološki kriminal – uporedna iskustva. *Strani pravni život* 53: 161–184.
12. Prlja, Dragan, Zvonimir Ivanović, Mario Reljanović. 2011. *Krivična dela visokotehnolokog kriminala*. Beograd: Institut za uporedno pravo.

Nataša Ranković*

IDENTITY THEFT AS A CRIMINAL OFFENSE: *DE LEGE LATA* AND *DE LEGE FERENDA*

Summary: The paper defines the basic forms of computer crime with an emphasis on identity theft as a special form that would de lege ferenda be characterized and adequately prescribed as a criminal offense in the Criminal Code of the Republic of Serbia. The aim of the work is to show the place of identity theft in the spectrum of various criminal acts that are classified as high-tech crime. The paper is divided into three parts, where the first is an introductory presentation describing the way in which the very rapid development of information and communication technologies affects the development of new methods for their abuse, after which the definitions of identity theft and its characteristics are described. The second part of the paper is dedicated to the ways, characteristics and modalities of identity theft, while the third part gave importance to the ways of protection and prevention of identity theft, within which a reasoned proposal was given for defining it in the Criminal Code of the Republic of Serbia. At the end of the paper, a short summary is given in the form of a conclusion.

Key words: *High-tech crime, Computer crime, Identity theft, Criminal Code, Crime*

* Author is an undergraduate student at the University of Belgrade – Faculty of Law, *natasarankovic24@gmail.com*. This paper was written under the mentorship of Ivan Đokić, Phd, assistant professor at the University of Belgrade – Faculty of Law, *djokic@ius.bg.ac.rs*