PRAVO
teorija i praksa

Godina XL **Novi Sad, 2023.** **Poseban broj**

IZDAVAČ/PUBLISHER:
PRAVNI FAKULTET ZA PRIVREDU
I PRAVOSUĐE U NOVOM SADU
UNIVERZITET PRIVREDNA AKADEMIJA
Geri Karolja 1, 21000 Novi Sad
Tel.: 021/400-484, lokal 109; 021/400-499

SUIZDAVAČ/CO-PUBLISHER:
„PRAVO" DOO
Novi Sad, Geri Karolja 1
21000 Novi Sad

Glavni urednik/Editor in chief:
Prof. dr Jelena Matijašević

Odgovorni urednik/Responsible editor:
dr Snežana Lakićević

Sekretar redakcije/Editorial secretary:
Prof. dr Nenad Stefanović

Lektor i korektor/Proofreader and corrector:
Mara Despotov

Lektor i korektor za engleski jezik/
Proofreader and corrector for the English language:
Jelena Dunđerski

Tehnička realizacija i štampa/Technical realization and print:
Graf 021, Novi Sad

Ovaj broj časopisa sufinansiran je od strane Pokrajinskog sekretarijata za visoko obrazovanje i naučnoistraživačku delatnost, na osnovu projekta od značaja za razvoj naučnoistraživačke delatnosti AP Vojvodine za projektni ciklus 2021-2024. godine pod nazivom "PROGRESIVNI RAZVOJ PRAVA U SAVREMENOM DIGITALNOM DRUŠTVU", i Ugovora o dodeli sredstava za finansiranje/ sufinansiranje projekata, AUTONOMNA POKRAJINA VOJVODINA, POKRAJINSKI SEKRETARIJAT ZA VISOKO OBRAZOVANJE I NAUČNOISTRAŽIVAČKU DELATNOST, br. 142-451-3134/2022-03.

LAW
theory and practice

Year XL **Novi Sad, 2023** **Special Edition**

CIP – Katalogizacija u publikaciji
Biblioteka Matice srpske, Novi Sad

34

PRAVO : teorija i praksa = Law : theory and practice / glavni urednik Jelena Matijašević; odgovorni urednik Snežana Lakićević. – God. 1, br. 1 (1984)– . – Novi Sad : Univerzitet Privredna akademija, Pravni fakultet za privredu i pravosuđe u Novom Sadu : „Pravo" doo, 1984–. – 24 cm

Tromesečno.

ISSN 0352-3713

COBISS.SR-ID 5442050

LAW – theory and practice
Year XL Novi Sad, 2023 Special Edition

C O N T E N T S

PROGRESSIVE DEVELOPMENT OF LAW IN THE MODERN DIGITAL SOCIETY

Dukić Mijatović S. Marijana
Uzelac N. Ozren
Stoiljković V. Aleksandra
Corporate social responsibility and sustainable development – international legal framework for goals achievement and some theoretical insights 1

Mirković Predrag
Digital assets – a legal approach to the regulation of the new property law institute 17

Mladenov Marijana
Human vs. Artificial intelligence - EU's legal response.....32

Golić Darko
Normative regulation of electronic administration in Republic of Serbia....44

Dragojlović Joko
Jurisdiction for criminal offenses of cybercrime – international and national standards.....63

Stojšić Dabetić Jelena
Wrap contracts and their influence on the contract law 84

Vasić Milica
Bulatović Petar
Digital transformation of the Business Registers Agency in the function of the modern digital society 99

PRAVO – teorija i praksa
Godina XL **Novi Sad, 2023.** **Poseban broj**

S A D R Ž A J

PROGRESIVNI RAZVOJ PRAVA U SAVREMENOM DIGITALNOM DRUŠTVU

Dukić Mijatović S. Marijana
Uzelac N. Ozren
Stoiljković V. Aleksandra
Društvena odgovornost i održivi razvoj – međunarodni pravni okvir za ostvarivanje ciljeva i neki teorijski uvidi 1

Mirković Predrag
Digitalna imovina – legislativni pristup regulisanju novog imovinskopravnog instituta 17

Mladenov Marijana
Ljudska protiv veštačke inteligencije – pravni odgovor EU 32

Golić Darko
Normativno uređenje elektronske uprave u Republici Srbiji 44

Dragojlović Joko
Nadležnost za krivična dela računarskog kriminaliteta – međunarodni i nacionalni standardi 63

Stojšić Dabetić Jelena
Wrap ugovori i njihov uticaj na ugovorno pravo 84

Vasić Milica
Bulatović Petar
Digitalna transformacija Agencije za privredne registre u funkciji savremenog digitalnog društva 99

Dukić Mijatović S. Marijana*
https://orcid.org/0000-0001-9535-2962
Uzelac N. Ozren**
https://orcid.org/0000-0001-6991-1644
Stoiljković V. Aleksandra****
https://orcid.org/0000-0002-4324-4537

UDK: 005.35:316.64
Original scientific paper
DOI: 10.5937/ptp2300001D
Received: 12.01.2023.
Approved on: 24.01.2023.
Pages: 1–16

CORPORATE SOCIAL RESPONSIBILITY AND SUSTAINABLE DEVELOPMENT – INTERNATIONAL LEGAL FRAMEWORK FOR GOALS ACHIEVEMENT AND SOME THEORETICAL INSIGHTS

ABSTRACT: Achieving a sustainable development should be one of the top priorities for the whole society. However, achieving a sustainable development is a complex function of different economic, social, institutional, political and historical factors. By implementing the corporate social responsibility, companies contribute to a sustainable development of the entire social system. According to the fact that it is not entirely clear at the micro level what corporate social responsibility involves, and that most of the company-level social activities are voluntarily initiated, it is necessary the institutional bodies encourage socially desirable forms of corporate behavior and implement the legal framework to business obligations to elicit responsible business procedures. Though responsible corporate business is highly desirable, companies have to consider the

* LLD, Associate professor, University of Novi Sad, The Faculty of Technical Sciences, Novi Sad, Serbia, e-mail: marijana.mijatovic@uns.ac.rs
** LLD, Assistant professor, University of Novi Sad, The Faculty of Economics in Subotica, Subotica, Serbia, e-mail: ozren.uzelac@ef.uns.ac.rs
*** LLM, Teaching Assistant, University of Novi Sad, Faculty of Economics in Subotica, Subotica, Serbia, e-mail: aleksandra.stoiljkovic@ef.uns.ac.rs

fact that the corporate interests and corporate social responsibility will always be constrained by the profit-maximizing prerequisites and general economic circumstances.

Keywords: *corporate social responsibility, sustainable development, business procedures, profit-maximizing orientation, legal framework.*

1. Introduction

Smooth and sustainable social development is a prerequisite for the stability and progress of the local, regional, and supranational political communities. It requires the economic, social and environmental dimensions to be achieved through the balanced and continuous progress of the national and international organizational units that corresponds to the rules and principles of the United Nations and other international organizations. Sustainable development (SD) is one of the top priorities for the national legislators that enact the country-specific regulations and implement defined international standards, rules and principles for sustainable local and regional development. Corporate Social Responsibility (CSR) is only one part of the stated ideal that economic and legal theory has stated in determining its content and defining it. Companies are becoming increasingly aware of the importance and impact they have on the environment in which they operate. If they want to be competitive, they should contribute to fulfilling the interests of their stakeholders. By implementing corporate social responsibility, companies not only have numerous benefits, but also contribute to national sustainable development.

Corporate Social Responsibility emerges as a new challenge in the light of the COVID-19 pandemic, and more than ever, it rises numerous concerns tightly connected to corporate social responsibility and sustainable development. We are witnessing a global interdependence, both at the company and national levels. Furthermore, there is a lack of classical interpretation of a company, having in mind its dual status as a legal entity and a profit-maximizing business entity. This paper treats some of these issues, aiming at analyzing the existing international legal framework for corporate social responsibility. Additionally, the paper highlights that the new reality requires CSR to be implemented just as an initial step toward sustainable development and overall social welfare.

The paper is structured as follows. After the introductory notes, the second section emphasizes the importance and benefits of corporate social

responsibility, the legal framework and the importance of institutions in achieving socially desirable forms of corporate behavior. The question is whether companies can behave socially unacceptable at all, or socially responsible, even when it is not required by law, having in mind that the modern business conditions imply competitiveness as the prerequisite of the long-term sustainability of companies.

The third section lists certain limitations in the implementation of corporate social responsibility, depending on the conditions and circumstances of a profit-oriented business. As Friedman states "The Social Responsibility of Business is to Increase its Profits" (Friedman, 1970) and companies must be careful when implementing the socially responsible activities. Namely, they should primarily pursue the corporate interests by making optimal economic decisions. On the other hand, society needs successful companies, those that not only prioritize responsible businesses, but also external activities that affect wider environment.

Finally, the fourth section concludes. In this regard, corporate social responsibility will be additionally regulated, not only within the companies and relations with the society as a whole, but also in defining business ethics, both in terms of maintaining existing economic activities and in choosing the future activities.

2. Is Corporate Social Responsibility a Choice, Obligation or Necessity in The Business of Today's Companies?

The undisputed goals of every social community are to meet the needs of its members, survival of the community and its development and improvement. The role of the way the system of management of social, economic and other areas of life functions is obvious. Democracy, the rule of law and the liberal economy stands out as the generally accepted model of the organization of modern society, which should guarantee the achievement of the above goals. However, how can a society resist and counteract the negative impact of excessive consumerism and the race for profit created by nothing but selfishness that leads to poverty and social exclusion of other members of society when the practice of socializing the capital losses of large businesses has settled? This inevitably raises a question about the morality of systems and institutions that should play a key role in preventing such phenomena. The last global financial crisis exposed this as a manifestation of when taxpayers, instead of financing programs of general interest to society, covered the consequences of other people's greed and disinterest in the common good

(Jovanović, 2012, p. 72). Thus, the minority in the financial power centers jeopardized the sustainable functioning of the state and deprived individuals and their families of the right and opportunity to enjoy the present and future due to unemployment, loss of social security and pensions (Jovanović, 2012, p. 72). Such events indicate that today's societies need to go a long way to the highest possible level of conscientiousness and honesty of decision-makers who can significantly influence the sustainable development of individuals' rights and social balance.

The behavior of individuals in society is governed by various norms: educational, customary and institutional (laws and by-laws). Legal rules of conduct are a special kind of so-called "obligatory" morality by which a society protects certain values or achieves its desired goals (Jovanović, 2013, p. 156). The extent to which the practice of acting under the norms of the law is an imperfect means of combating the irresponsible social behavior of business entities can also be seen from the fact that the use of a fact or condition to obtain an advantage in the market may not always be contrary to the law.

There are many examples of socially irresponsible behavior of businesses such as cheating consumers, investors, government institutions, exploiting and mobbing employees, putting consumers in dangerous situations, polluting the environment, etc. Socially irresponsible behavior of an economic entity is determined by applying certain standards of guaranteed rights (right to a healthy environment, right to consumer protection, etc.) and general legal principles (the principle of conscientiousness and honesty, the principle of prohibition of abuse of rights and other legal and other principles), coercive and other regulations and codes of conduct in relation to the disputed facts.

Campbell (2007), in his Institutional Theory on Corporate Social Responsibility, stresses the importance of institutions in achieving the goal of market participants behaving socially responsible, while also bearing in mind the free-market institutions whose inadequate functioning was the cause of the global financial crisis that erupted at the end of 2007. We believe that this theory is due to the nature of the liberal economic system, in which it is considered that the role of the state in the market should be minimal. Consequently, this means that all third parties interested in the business of corporations are left to the conscientiousness and morality of their corporate governance and business procedures, which, after the outbreak of the global financial crisis, was seen as a key issue. The same author plastically explains that if corporations are to maximize profit and share value, then it is logical that corporations will do anything to achieve this goal, perhaps by acting in

socially irresponsible ways if they think they will go unpunished (Campbell, 2007, p. 946). In legal theory, there are occasional attempts to illustrate CSR behavior with specific examples. For example, in the field of business of an insurance company, the legal theory points out that socially responsible and moral conduct of insurance companies entails abstaining from certain actions (refraining from discriminating against the insured regarding the possibility of concluding insurance under certain insurance conditions, refraining from the unreasonable delay with payment insurance premiums, etc.) (Jovanović, 2013, p. 163). We believe that the above examples of unacceptable behavior in the insurance industry cannot be the only ones by which the corporate social responsibility of insurance companies is measured, because it is much broader and depends on the specific circumstances. It should be borne in mind that efforts to maintain or expand insurance coverage can also be seen as positive behavior by insurance companies, which thus extend the distribution of socially valuable and useful goods and contribute to collective well-being (Stone, 2002, p. 70). Likewise, citing individual examples of socially irresponsible behavior in other economic-legal relationships certainly cannot constitute a definitive list of all possible manifestations of such behavior by economic entities.

In legal theory, Porter and Kramer emphasize that corporate social responsibility should not be the result of tensions, but its manifestation should be sought in the interdependence of firms and society (Porter & Kramer, 2006, p. 5). According to him, interdependence manifests itself as a link that acts two-way through the impact of the firm's business on the company and through the influence of social conditions on the realization of the company's strategy and its overall business. Under social conditions, it entails four basic categories: the first are quantitative and qualitative business conditions (available workforce, transport, infrastructure, etc.), the second is a legal framework that affects competition (in relation to intellectual property, transparency, combating corruption and fostering investment), the third is the size and sophistication of local demand (influenced by the product quality and safety standards, consumer rights and fairness in public procurement) and the fourth is the existence of an accompanying industry and machine manufacturer (Porter & Kramer, 2006, p. 6).

Socially responsible business practices in companies represent a concept according to which economic entities consciously and voluntarily dedicate themselves to activities in order to have a positive impact on their work, social and natural environment. This behavior is a consequence of developing an awareness of the importance that companies have in modern society (Aleksić,

Komazec & Stoiljković, 2017, p. 9). CSR has been used as a synonym for business ethics, defined as tantamount to corporate philanthropy, and considered strictly as relating to environmental policy (McWilliams, Siegel & Wright, 2006, p. 8). Modern business philosophy assumes that an organization must be responsible for its actions and deeds that affect all active members of the community. Companies that want to be competitive should satisfy the interests of a large number of interest groups operating within a particular business environment (Ćeha, 2013, p. 1). The need to balance the content and scope of corporate social responsibility was aided by the positively formulated definition of the International Organization for Standardization. This definition defines the content of social responsibility not only of economic entities but also of groups of persons with easily identifiable competences, authorities and goals. According to this definition, social responsibility is the responsibility of an organization or group of persons for positive or negative changes in society, economy or environment that are wholly or partly due to decisions and activities of the past or present through transparent and ethical behavior that: – contributes to sustainable development, including the health and well-being of society; takes into account the expectations of stakeholders; which is in accordance with positive regulations and international standards of behavior; and which is integrated throughout the organization and applicable to the relationships it enters into (International Organization for Standardization, sec. 2.18). The above definition covers four important assumptions of corporate social responsibility, namely: sustainable development of society, protection of interested parties (for example, consumers), the legality of concrete behavior and adaptation of corporate organization to the principles of corporate social responsibility. We believe that the essential prerequisites for achieving the set goal are thus covered. The aforementioned assumptions also represent the obligations of the legislative and supervisory-regulatory bodies in adopting regulations, adopting rules and supervising them, as well as all other institutions and economic entities that they must implement when satisfying individual interests (consumer protection and profit-making – authors note).

Today's organizations are immersed in a global market, where any detail can provide a competitive advantage over rival companies and condition their sustainability (Herrera & de las Heras-Rosas, 2020, p. 841). CSR is becoming increasingly important for business organizations. It is clear that this is going to become a standard in business, having in mind that EU commission created a certain number of directions, there is already presented ISO standard 26000 related to the social responsibility, and also many other benefits that CSR can bring to the business and wider community and environment (Grubor, Berber,

Aleksić & Bjekić, 2020, p. 9). According to Van Marrewijk the philanthropic approaches might be the roots of CS, but the different approaches to corporate responsibility clearly show that CSR is a new and distinct phenomenon. Its societal approach especially appears to be a (strategic) response to changing circumstances and new corporate challenges that had not previously occurred (Van Marrewijk, 2003, p. 3). Modern management emphasizes that one of the obligations of business institutions is to engage in solving certain social problems that are outside their usual field of activity if they have the knowledge and experience to solve them (Certo & Certo, 2008, p. 51).

Business practices of the world's most successful corporations show that there is a high degree of correlation between the positive opinions of interest groups within the company and the quality of business (Ćeha, 2013, p. 9). Corporate responsibility as strategic determination of business increases financial performance of company, decreases some costs, reinforces ethical behaviour and job satisfaction, and enhances business reputation (Knežević & Mijoković, 2017, p. 31). Accordingly, in recent years, CSR activities have been recognized as a natural obligation of firms. As sustainable management has become much more important, firms have begun to recognize CSR internally as an important business strategy (Cho, Chung & Young, 2019, p. 1). Enterprises become aware that a corporate social responsibility can be used as a strategy to foster sustainable development of enterprises (Jarmuševiča & Iliško, 2019, p. 82). The responsibility of a company towards environment strengthens its reputation, increases the value of corporate brand and ensures long-term sustainable development (Mandarić & Milovanović, 2016, p. 412). The companies that establish a symbiosis between the principles of profitability and social responsibility have long-term growth prospects (Krivokapić, 2014, p. 281).

Realizing the importance the corporate social responsibility has for the business development, the biggest challenge facing the modern organizations is to develop politics and practices in the CSR area and to successfully implement them into the organization's corporate development strategy (Petrov-Stoyanov, 2018, p. 728). Business organizations face globalization processes and related economic competition, technological change as well as new cultural models, notably, those related to sustainable development, the dynamics of social networks and the knowledge society. They are not only at the forefront of numerous social transformations but are also compelled to change their own perspectives and to integrate, either voluntarily or under external pressure, new concerns, such as CSR and sustainable development, which are now widely recognized at the international level (Sales, 2019, p. 3). In order to move CSR from the zone of voluntarism to the zone of obligation, it

is necessary to institutionally define and achieve a balance between economic, environmental and social imperatives (Drašković & Lojpur, 2014, p. 20).

3. Some Limitations and Business Implications of CSR Implementation

Implementation of sustainable development according to the UN Resolution "The Future We Want" (United Nations, 2012) depends on the active engagement of both the public and private sectors. The resolution emphasizes the special role of national regulatory and policy frameworks that enable business and industry to advance sustainable development initiatives, while the private sector should engage in responsible business practices (United Nations, 2012, p. 46). Also, the Resolution affirms the importance of corporate sustainability reporting and states that listed and large companies in particular should consider integrating sustainability information into their reporting cycle (United Nations, 2012, p. 47).

The above-mentioned UN recommendations are covered at EU level in the form of regulations that had to be implemented by EU Member States several years ago (Directive 2014/95/EU), to further elaborate on how to implement it later on by the European Commission with its implementing regulation. Probably given that large businesses have a decisive influence on the sustainability of development, and referring to the aforementioned UN Resolution of 2012, the 2014 EU Directive stipulated that the obligation to report facts necessary to understand their development, performance, position and impact of business at least in relation to the environment, impact on society and employees, respect for human rights, and anti-corruption issues are experienced by large companies, joint-stock companies and public enterprises with an average of 500 employees during the financial year. It is non-financial reporting that can be an integral part of the regular financial and operating reports or in the form of stand-alone reports. Also, these reports should not deal with the overall business and all circumstances of the business entity, but only those that were relevant to sustainable development in the reporting year. Recognizing the reasons why SMEs (small and medium-sized enterprises) and entrepreneurs are exempt from this obligation, the question arises as to whether and to what extent they can decisively influence the fastness of sustainable development? Can any of them in their business lead to environmental pollution or otherwise impair the interests of others? We believe that the answer to the question posed is far from certain, given that large enterprises have a decisive influence on all aspects of corporate social

responsibility, and that entrepreneurs, small and medium-sized enterprises, do not have this importance (Guidelines on non-financial reporting, 2017).

Based on the insight into selected international legal sources, certain conclusions can be drawn. Failure to prescribe more precise obligations with respect to desirable – corporate responsible behavior, apart from the summary reporting obligation as assessed by the business entity, seems to leave much room for omitting or distorting negative facts and circumstances. Apart from the aforementioned, given that the views expressed in the resolutions of the UN General Assembly are, by their nature, recommendations for action, and that the rules of the aforementioned EU Directive 2014 do not regulate many other issues of social development, there are a number of areas (activities of various associations, providing humanitarian assistance, assistance in cases of natural disasters, support for civil initiatives or actions, etc.) in which corporate social responsibility remains a matter of goodwill of corporate governance whose decisions are limited by the interests of shareholders. It is precisely the shareholder-oriented attitude that is problematic in the shareholder form of capitalism, and even more so in relation to corporate social responsibility (Smith, 2011). Pelgrin described this problem in the business of reinsurance companies, which states that relativistic ethical guidelines that emerge from the inside out (ethics, interpretation and treatment in the way understood by corporate governance in external interactions – authors note) are aimed at improving financial business and management efficiency, not to apply an ethical approach inherent in an individual, organization, and society in open systems (Pelgrin, 2008, p. 15). In any case, corporate social responsibility will always be limited by the conditions and circumstances of a profit-oriented business, with corporate social responsibility still dependent on the corporate governance conscientiousness and ethics. It will primarily take into account the corporate interest that cannot be the victim of economically irrational decisions. In the market economy and extreme competition in the global market, economic motives play an important, and perhaps even the most significant role in making decisions on the implementation of socially responsible activities, which is totally understandable. After all, companies are profit organizations, and it is illogical to expect from them to take actions that are inconsistent with the goal of achieving positive financial results (Stojanović-Aleksić & Bošković, 2016, p. 1383). Social activities, as a rule, are useful and achieve certain social goals, but it is not realistic to expect that their financing is fully borne by socially responsible companies. There is still intensive discussion whether business schools have failed to incorporate enough of business ethics and a deep understanding related to real-world responsibilities (Blomkvist &

Uppvall, 2008, p. 58). However, we believe that corporate social responsibility must be respected to the greatest extent possible when it comes to protecting human rights and protecting the environment.

In addition to the above, one should also bear in mind the conclusions of economic theory regarding the definitions and possibilities of achieving corporate social responsibility. Thus, attempts were made to measure the degree of comparative corporate social responsibility in a number of countries in business practice, and it was concluded that the prevailing definitions of corporate social responsibility were not suitable as a basis for comparative measurement (Gjølberg, 2009, p. 12), that the statistics on the relationship between corporate social responsibility and corporate financial performance are too variable and fragmented to draw any general conclusions (Orlitzky, Schmidt & Rynes, 2003). Attempts to measure or compare corporate social responsibility are likely to remain only an unfulfilled goal due to the large number of variables in terms of data and methodology.[1] The literature also cites one reason why it is not always realistic that corporate social responsibility will be manifested in the right way. It is a matter of passing on the social costs associated with any activity, product or service to customers through their higher prices (Certo & Certo, 2008, p. 51), which is certainly not acceptable for consumers and for companies that may lose competitiveness on the market.

4. Conclusions

The idea of sustainable development relies on the existence of a constantly evolving society in order to preserve social cohesion and peace. In achieving this objective, national legislators must implement properly selected policies at the local and regional levels that are also harmoniously integrated at the national and international levels. The National Assembly

[1] Some of the variables are: The Dow Jones Sustainability ™ Europe Index, which consists of 20% of Europe's largest corporate leaders out of 600 in the area of corporate social responsibility according to the S&P Global BMI (Standard and Poor's Global Broad Market Index) based on long-term economic, environmental and social criteria. Available online: https://eu.spindices.com/indices/equity/dow-jones-sustainability-europe-index (accessed on 01/10/2021); The WBCSD (The World Business Council for Sustainable Development) made up of CEOs from over 200 companies working for sustainable development by advocating for best business practices in corporate responsibility. Available online: https://www.wbcsd.org/Overview/About-us (accessed on 01/10/2021) and the UN Global Compact, an initiative of over 11,500 companies, non-governmental organizations, universities, UN bodies and labor unions, with a view to achieving 10 basic principles in the fields of human rights, labor relations, protecting the environment and fighting corruption. This is an initiative of the UNSecretary-General. Available online: https://www.unglobalcompact.org/ (accessed on 01/10/2021).

should pass appropriate legislative and appropriate budgets, whereas the executives should effectively implement the prescribed obligations in cooperation with local/regional governments, national and international institutions and organizations. Such a legal framework must highlight the role and comparative advantage of an adequately organized and coordinated system in achieving sustainable development within a country. However, the legal framework itself is not a guarantee of achieving the predefined goals without an effective and substantive implementation that can deliver the intended results.

Companies are facing globalization, increasing competition and various pressures from consumers, NGOs, etc., which in a way forces them to behave socially responsible. By implementing corporate social responsibility through the socially oriented activities, companies can achieve numerous benefits such as better reputation, increasing financial performance, long-term growth and business sustainability. The company-level voluntary social activities are very important for achieving sustainable development; however, society cannot rely only on the willingness of the companies, and it is necessary to move CSR from the zone of voluntarism to the zone of obligation.

Corporate social responsibility in the implementation of the legal framework for harmonious sustainable social development is primarily about the obligation of business entities to adopt and implement responsible business procedures. They must reconcile the interests of an economic entity with the interest of national development. Bearing in mind frequent disinterests of the business entities in undertaking socially responsible measures, the role of institutional bodies should be more pronounced through the sophisticated incentives for socially desirable forms of corporate behavior. This kind of practice will propagate from the micro-level to the national level and have a positive impact on sustainable development of the Republic of Serbia.

We believe that the Republic of Serbia should follow the rules and standards of the European Union, including the 2014 Non-Financial Reporting Directive and pay a special attention to large enterprises and their impact on aspects of corporate social responsibility. On the other hand, entrepreneurs, and the small and medium-sized enterprises do not have such a huge impact on the economy and should not be unnecessarily overwhelmed by these obligations.

Dukić Mijatović S. Marijana
Fakultet tehničkih nauka, Univerzitet u Novom Sadu, Srbija

Uzelac N. Ozren
Ekonomski fakultet u Subotici, Univerzitet u Novom Sadu, Srbija

Stoiljković V. Aleksandra
Ekonomski fakultet u Subotici, Univerzitet u Novom Sadu, Srbija

DRUŠTVENA ODGOVORNOST I ODRŽIVI RAZVOJ – MEĐUNARODNI PRAVNI OKVIR ZA OSTVARIVANJE CILJEVA I NEKI TEORIJSKI UVIDI

REZIME: Postizanje održivog razvoja trebalo bi da bude jedan od glavnih prioriteta celog društva. Međutim, postizanje održivog razvoja je složena funkcija različitih ekonomskih, društvenih, institucionalnih, političkih i istorijskih faktora. Sprovođenjem društveno odgovornog poslovanja kompanije doprinose održivom razvoju celokupnog društvenog sistema. S obzirom na to da na mikro nivou nije sasvim jasno šta je korporativna društvena odgovornost i da se većina društvenih aktivnosti na nivou kompanije pokreće dobrovoljno, neophodno je da institucionalni organi podstiču društveno poželjne oblike korporativnog ponašanja i primenjuju zakonski okvir na poslovne obaveze i time da izazovu primenu odgovornih poslovnih procedura. Iako je odgovorno korporativno poslovanje veoma poželjno, kompanije moraju da uzmu u obzir činjenicu da će korporativni interesi i korporativna društvena odgovornost uvek biti ograničeni preduslovima za maksimiziranje profita i opštim ekonomskim okolnostima.

Ključne reči: *korporativna društvena odgovornost, održivi razvoj, poslovne procedure, orijentacija ka maksimizaciji profita, pravni okvir.*

References

1. Aleksić, M., Komazec, Lj., & Stoiljković, A. (2017). Promocija korporativnih i društvenih cljeva u funkciji održivog razvoja primer R. Srbije. [Promotion of corporate and social values in the function of sustainable development, example of the Republic of Serbia]. In:*Menadžment i marketing – trendovi i uticaji na efikasnost tržišta Republike Srbije* [Scientific Conference*Management and Marketing – trends and impacts on the efficiency of theRepublic of Serbia market*] (pp. 1-10), Subotica: Ekonomski fakultet u Subotici
2. Blomkvist, P., & Uppvall, L. (2012). A Chain is only as Strong as its Weakest Link: Managing Change in the Curriculum of Industrial Management Education. *International Journal of Industrial Engineering and Management* (IJIEM), *3(2*), pp. 53-65. Downloaded 2021, October 02 from http://www.ijiemjournal.org/images/journal/volume3/ijiem_vol3_no2_2.pdf
3. Campbell, L. J. (2007). Why would corporations behave in socially responsible ways? An institutional theory of corporate social responsibility. *Academy of Management Review*, *32*(3), pp. 946–967. DOI:10.5465/amr.2007.25275684
4. Ćeha, M., (2013). Analysis of the Application of the Concept of Corporate Social Responsibility in Local Businesses. *The European Journal of Applied Economics*, *10*(1), pp. 1-10. DOI: 10.5937/sjas1301001C
5. Certo, C. S., & Certo T. S. (2008). *Moderni menadžment* [*Modern management*]. Zagreb: Mate
6. Cho, S. J., Chung, C. Y.,& Young, J. (2019). Study on the Relationship between CSR and Financial Performance. *Sustainability*, *11*(2), pp. 343. https://doi.org/10.3390/su11020343
7. Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups. *Official Journal of the European Union*, L 330, 15.11.2014, pp. 1-9
8. Drašković, V., & Lojpur, A. 2014. Corporate social responsibility: Illusion vs. real possibility, voluntarism vs. compliance. *Strategic Management*, *19*(1), pp. 16-21.
9. Friedman, M. (1970). *The New York Times Magazine*, September 13
10. Gjølberg, M. (2009). Measuring the immeasurable? Constructing an index of CSR practices and CSR performance in 20 countries. *Scandinavian Journal of Management,25*(1), pp. 10–22. DOI: 10.1016/j.scaman.2008.10.003

11. Grubor, A., Berber, N., Aleksić, M., & Bjekić, R. (2020). The influence of corporate social responsibility on organizational performances: A research in AP Vojvodina. *Anali Ekonomskog fakulteta u Subotici*, *56*(43), pp. 3-13. DOI:10.5937/AnEkSub2001003G
12. Guidelines on non-financial reporting (methodology for reporting non-financial information). *Official Journal of the European Union*, C-215, 5.7.2017, pp. 1–20.
13. Herrera, J., & de las Heras-Rosas, C. (2020). Corporate social responsibility and human resource management: Towards sustainable business organizations. *Sustainability*, *12*(3), pp. 841-865. https://doi.org/10.3390/su12030841
14. International Organization for Standardization. *ISO 26000:2010(en) – Guidance on social responsibility*. Geneva: ISO/TMB Working Group on Social Responsibility. Downloaded 2021, October 05 from https://www.iso.org/obp/ui/#iso:std:iso:26000:ed-1:v1:en
15. Jarmuševiča, V., & Iliško, D. (2019). The politics of a corporate social responsibility in the enterprise x for a sustainable regional development. In: *Proceedings of the 61th International Scientific Conference of Daugavpils University* (pp. 82-91), Daugavpils: Daugavpils University
16. Jovanović, S. (2012). Aristotelovi postulati društvenog uređenja kao uzor za modernu organizaciju države [Aristotle'a postulates of social organization as a model for modern state organization]. *Pravo – teorija i praksa*, *29*(7–9), pp. 71–84
17. Jovanović, S. (2013). Moralnost u osiguranju i društveno odgovorno ponašanje – Stvarnost ili cilj kojem se teži [Morality in insurance and socially responsible behavior – Reality or aspirational goal]. In: Marano, P., Jovanović, S., Labudović Stanković, J. (urednici),*Pravo osiguranja Srbije u tranziciji ka evropskom (EU) pravu osiguranja* [Serbian insurance law in transition to European (EU) insurance law] (pp. 155-168). Beograd: Udruženje za pravo osiguranja Srbije
18. Knežević, G., & Mijoković, M. (2017). Sustainability reporting of listed companies on the Belgrade stock exchange. In: *Challenges in Modern Corporate Governance: book of proceedings* (pp. 30-35). Belgrade: Singidunum University, DOI: https://doi.org/10.15308/finiz-2017-30-35
19. Krivokapić, S. (2014). Analysis of the level of alignment of marketing objectives with social responsibility in the countries in transition. In: Marković, A., Barjaktarović Rakočević, S. (eds.), *New Business Models and Sustainable Competitiveness: symposium proceedings*(pp. 281-286). Belgrade: Faculty of organization science

20. Mandarić, M., & Milovanović, V. (2016). The Role of CSR in the Development of Sustainable Tourism in Serbia. In: *TISC – Tourism International Scientific Conference* (pp. 412-429),Vrnjačka Banja
21. McWilliams, A., Siegel, D. S., & Wright, P. M. 2006. Corporate social responsibility: Strategic implications. *Journal of management studies, 43*(1), pp. 1-18. https://doi.org/10.1111/j.1467-6486.2006.00580.x
22. Orlitzky, M., Schmidt, L. F., & Rynes L. S. (2003). Corporate Social and Financial Performance: A Meta-analysis. *Organization Studies*, *24*(3), pp. 403–441. https://doi.org/10.1177/0170840603024003910
23. Pelgrin, T. (2008). Promena prirode industrije reosiguranja – poziv na etičko postupanje [The changing nature of the reinsurance industry – a call for ethical action]. *Revija za pravo osiguranja*, *7*(3), pp. 13–19
24. Petrov-Stoyanov, P. (2018). The impact of corporate social responsibility in building the corporate strategy. In: *Proceedings of 2nd International Scientific Conference on Recent Advances in Information Technology, Tourism, Economics, Management and Agriculture–ITEMA*. (pp. 728-734). Graz, https://doi.org/10.31410/itema.2018.728
25. Porter, E. M., & Kramer, R. M. (2006). Strategy and Society: The Link between Competitive Advantage and Corporate Social Responsibility. *Harvard Business Review*, *84*(12), pp. 78-92. Downloaded 2021, October 01 from https://hbr.org/2006/12/strategy-and-society-the-link-between-competitive-advantage-and-corporate-social-responsibility
26. Sales, A. (2019). The Institutionalization of the Domain of Corporate Social Responsibility. In: Sales, A. (ed.), *Corporate Social Responsibility and Corporate Change* (pp. 3-41). Springer International Publishing
27. Smith, E. R. (2011). *Defining Corporate Social Responsibility: A Systems Approach for Socially Responsible Capitalism*: *Master of Philosophy Theses*. Pennsylvania: University of Pennsylvania. Downloaded 2021, October 01 from http://repository.upenn.edu/od_theses_mp/9 (01/10/2021).
28. Stojanović-Aleksić, V. & Bošković, A. (2016). Corporate social responsibility: philanthropy, obligation or utilitarianism? In: *Reshaping the Future through Sustainable Business Development and Entrepreneurship: XV International Symposium Symorg 2016* (1382-1388). Belgrade: Faculty of organization science
29. Stone, D. (2002). Beyond Moral Hazard: Insurance as Moral Opportunity. Baker, T. & Simon, J. (eds.), In: *Embracing Risk – The Changing Culture of Insurance and Responsibility* (pp. 52-79). Chicago & London: The University of Chicago Press

30. United Nations Global Compact. Downloaded 2021, October 01 from https://www.unglobalcompact.org/
31. United Nations. 2012. *Resolution adopted by the General Assembly on 27 July 2012 66/288. The future we want*. New York: United Nations
32. Van Marrewijk, M. (2003). Concepts and Definitions of CSR and Corporate Sustainability – between agency and communion. *Journal of Business Ethics*, *44*(2/3), pp. 95–105
33. World Business Council for Sustainable Development. Downloaded 2021, October 01 from https://www.wbcsd.org/Overview/About-us

Mirković Predrag[*]
http://orcid.org/0000-0003-2323-040X

UDK: 347.7:004
Original scientific paper
DOI: 10.5937/ptp2300017M
Received: 02.02.2023.
Approved on: 25.02.2023.
Pages: 17–31

DIGITAL ASSETS – A LEGAL APPROACH TO THE REGULATION OF THE NEW PROPERTY LAW INSTITUTE

ABSTRACT: Development of a digital technology has transformed the way in which an individual, a social group or community, i.e. a state, interacts in their domains of interest. The application of a digital technology, especially ICT, has caused the need to review whether the existing legislative solutions correspond to such news, or whether it is necessary to change or supplement the legal system of the state with new regulations. One of such issues refers to the creation of new types of assets identified as digital assets or the assets based on the creation of a digital technology. The subject of the research paper is the analysis of the institute of digital property with a special reference to the legislative domain of the way of issuing digital property. In his work, the author affirmed the issue of the importance of the legislative challenge in the standardization of relevant social phenomena and relations in the age of the intensive development and application of a digital technology. The aim of the work was achieved in the domain of the conducted normative analysis of the relevant provisions of the Digital Property Act in the part referring to the legislative approach to standardizing the concept of the digital property institute, as well as the particular issues from the domain of issuing digital property.

Keywords*: digital society, digital economy, digital assets, digital token, digital assets issuance.*

---

[*] LLD, Associate Professor, Faculty of Law for Commerce and Judiciary in Novi Sad, Republic of Serbia,e-mail: mirkovic@pravni-fakultet.info

1. Introduction

Digital transformation of modern society caused by the development of new technologies presents the State with the challenge of regulating its status and usage. Although it is unquestionable that digital society acquires significant range of benefits from the daily usage of new technologies, especially those that belong to information and communication technologies (ICT), the State is at the same time interested in regulating the new social reality by innovating existing legal solutions, i.e. by adopting new laws. The development of digital society during the last twenty years has functionally changed and influenced all aspects of a society, as well as the individual within it. The application of digital technology, especially ICT, has caused the need to review whether the existing legislative solutions correspond to such novelties, or whether it is necessary that the legal system of the State be changed and supplemented with new regulations. One such issue is the creation of a new type of property that is identified as digital property or property created as a result of the usage of digital technology. The Republic of Serbia is one of the first countries that systematically regulates this new reality – the existence of digital property as a new legal institution of property law. With the adoption of the Digital Property Act, a regulation was incorporated into the legal system of the Republic of Serbia, which represents the most innovative legal act that normatively addresses what already exists in practice and real life, namely a new form of property created as a result of the use of digital technology.

The subject of the research paper is the analysis of the institute of digital property with special reference to the legislative regime of issuing digital property. The goal of the paper is to determine, based on the analysis of the relevant provisions of the Digital Property Act, how the concept of digital property is defined. As a result, deductive conclusions in the domain of general and special characteristics of digital property as legal creation are derived from normative analysis. The specificaim of the research is to determine the legislative correlation in the domain of the legislative approach to the regulation of the issuance of digital assets and financial instruments. The realization of the research objectives will determine the legislative approach to the regulation of the institute of digital property, as a new institute of property law. The justification of the research subject is based on the absence of scientifically relevant research in the field of analysis of the Digital Property Act, and the author's intention is to contribute to higher level of scientific and professional awareness with this paper.

Analysis of the content of the Digital Property Act is the primary methodological approach to the research of the subject of the paper, with limited usage of relevant literature sources. The normative research method is the primary research method, since there are significant limitations in terms of scientific and professional literary sources in the domain of the research subject.

2. The emergence and development of digital society as a prerequisite for the creation of digital property

The development of digital technology has transformed the way an individual, social group. other community or the state interact in their domains of interest. Modern society is defined as a digital society if the process of acceptance and inclusion of digital technology is included at every level. Digital society is characterized by a specific social structure – a network, which functions on the basis of network logic and is strengthened by digital technologies. The theoretical foundations serve as a background for the analysis of the impact of spatial transformation in the network society, as the change of place and space of digitally networked learning (Castells, 2000, p. 43). A digital society is a society that uses new technologies for the realisation of its professional and personal needs, and information and communication technologies are at the center of that process. Such societies need adequate legal security in the digital space, which is one of the most important global issues today. The concept of digital property is a conceptual phenomenological question, since few legal systems in the world define its concept. In the broader concept of understanding, the concept of digital property is functionally connected with the usage of a certain digital technology in creating a certain digital record of a different character that has a certain value in the digital space, its named owner and which as such can be the subject of purchase, exchange or sale.The best example of what is referred to as a digital property today is the emergence of bitcoin as one of the first forms of what in a broader context of importance can be referred to as a digital property. Society, in which ICT plays a key role, is often called the information society. It is a society characterized by a very high intensity of information circulation in the everyday life of most people, including economic subjects. It can be stated that a given society is characterized by the usage of general or compatible technologies for easy and efficient realization of a wide range of personal, social, educational and business activities (Stojšić Dabetić & Mirković, 2021, pp. 135-147). The influence of digital technologies on social changes

is undeniably dominant and significant, but within one society, changes do not occur linearly in all spheres of society, but particularly from area to area. The area of the economy of a society, i.e. the state, in a given process was, and still is, under the significant influence of these factors, so today's modern society is a society that has created a new economy on a global level, a digital economy (Stojšić Dabetić, Mirković, 2022).However, during last two decades, states and international economic organizations have been faced with the issues of finding an adequate approach in the legal regulation of general and particular issues that arise within the concept of what we call the digital economy, within which the issue of legal regulation of digital property is also beginning relevant. These issues are equally challenging, both from the point of view of the national legal systems of the states, and from the point of view of international regulation (Dukić Mijatović & Mirković, 2022, pp. 54-55). The role of the state is to create a legislative framework that will serve to protect the interests of economic entities, in order to achieve business security as a general concept. The issue of regulation from the aspect of legislation is an interesting issue for the state in every segment of social interaction. (Stojšić Dabetić & Mirković, 2022). Accordingly, the digital economy is the economy of the present and not of the future, based on the application of various technical and technological solutions within what is defined as the economy, while within it the issue of legislative regulation of new economic values arises, of which the emergence or creation of digital property is particularly demanding one, as a new legal institute that must be legislatively defined and determined. As such, it was created as a direct consequence of the development and application of digital technology, and as such it was not recognized within the traditional understanding of property as an economic and legal value until now. Consequently, the necessity of adopting or revising existing legal regulations is an interesting question from the perspective of the state as a legislator. This issue goes beyond national legal frameworks, so there are significant legislative activities of international organizations at the regional or global level.

3. Digital property as legal institute in the national law

Digital property, as a special type of asset, is considered one of the biggest challenges of modern property law (Jovanović, 2021). It is precisely the almost unlimited potential of applying digital assets in the future, as well as economy and efficiency are the main reasons for the increased interest of legislators around the world and numerous international financial

organizations for this type of asset. Economy and efficiency are achieved primarily by eliminating intermediaries in carrying out transactions (banks, companies that provide payment card services, etc.), which undoubtedly significantly reduces total transaction costs and enables faster realization of monetary transactions (Mihajlović, 2021). Based on that, a new property law institute, digital property, is being created. The question of its standardization is raised as a question of the necessity for legislative regulation, both at the national and international level.

Digital Property Act is the first regulation of a systemic character that defines the institute of digital property. Digital property, i.e. virtual property, means a digital record of value that can be digitally bought, sold, exchanged or transferred and that can be used as a medium of exchange or for investment purposes, whereby digital property does not include digital records of currencies that are legal currency and other financial assets that are regulated by other laws, except when otherwise regulated by this law (Digital Property Act, 2020). The domestic legislator had extremely demanding tasks, not only in the conception of this regulation, but in defining a number of new concepts within the wording of the law. The fact that the legislator defines over 40 terms used speaks in favor of the legislative innovation of the regulation itself. Adequate definitions of various terms in the text of the law were particularly demanding due to the absence of comparative legal solutions in the given domain. True, its adoption is relevant in connection with the publication of the Proposal for an EU Regulation on cryptoasset markets, although the national law deviates to a large extent from the solutions contained in the Proposal for Regulation 7, trying to find its own (original) path of development in this innovative area (Mihajlović, 2021).

The main features of the concept of digital property according to the legal definition are the following. First, the legislator equates the concept of digital property with virtual property. The reason for this is the extension of the application of the given legal solution to the broader context of the reality of different ways of creating digital property. Such solutions are adequate, having in mind the technological diversity of digital property creation. In addition, the legislator specifically highlights that this type of "new property law institute" arises within the digital space through different mechanisms of creation, which also represents the classification of digital property. A digital or virtual property is an asset based on a digital record. The method of creation of this type of property is necessarily defined in the term and the legislator does so adequately. In this way, an additional distinction is made between the concept of digital property and other forms of property. Since the legislator

uses the term "digital record", there is a need to define the concept of this type of property more closely. Namely, a digital record is any record of a digital character that can be software, hardware or a combination of both. For this reason, it is quite clear that not every digital record can be treated as a digital property. The legislator defined that it is a digital record of value, making it clearly normatively distinct from other digital records. Although there is still no universally accepted terminology and definitions of basic terms related to this technology, there is agreement on its basic features: 1) decentralization – which implies the absence of a central database in which records are made; 2) distributedness – which gives the opportunity to all members of the digital network to participate in the process of confirming specific transactions carried out between functioning, especially in terms of providing security to market participants, it is necessary to use different cryptography techniques (computer-based encryption techniques in order to confirm transactions and store data about property, its owners, participants in transactions, etc.; the most commonly used encryption techniques are public and private cryptographic keys.

A digital record of value represents a narrower concept of digital or virtual property. Since it represents property, the issue of its legal treatment in legal transactions is absolutely necessary. Digital property can be bought, sold, exchanged or transferred digitally. It is important to understand the legislator who, within the framework of defining the concept of digital property, makes a series of language formulations necessarily specific to this form of property. We recognize the fact that this form of property can be traded digitally, which on the one hand represents a limitation in the domain of the way in which it is traded, while on the other hand it represents a clear distinction in relation to the circulation of other forms of property. The legislator also foresees a wider range of rights that belong to the holder of digital property, although we believe that it was not necessary to define it explicitly. Digital property can be used as a means of exchange or for investment purposes, which intentionally indicates that this form of property is suitable for investment of an economic nature. An interesting specificity of the way of defining the concept of digital property is the legislator's intention to separate two concepts that are often identified as identical in the social context, the concept of digital property and the concept of virtual currency.The reason for this legal solution is based on the still unsettled understanding of the difference between digital property on one hand, and virtual currencies on the other. The legislator additionally explaines the legislative difference in the context of clear definition of the concept of virtual currency in item 2, article 2 of the Act. However, the

legislator treats the existence of two forms of virtual currencies. Within Article 2 point 1 of the Act, it is defined that digital property does not include digital records of currencies that are legal means of payment regulated by another law. In terms of this Act, digital currency is a type of digital property, which means that the concept of digital property is a higher-order concept. Virtual currency is a type of digital property that has not been issued and its value is not guaranteed by the central bank or other public authority, which is not necessarily connected to legal means of payment and does not have the legal status of money or currency, but is accepted by natural and legal persons as a means of exchange and can be bought, sold, exchanged, transferred and stored electronically (Digital Property Act, 2020). It clearly follows from the above that the concept of digital property is a concept of the highest order that includes different forms or types of digital property that are identified within the framework of this Act.Since digital currency records may be legal currency, they are not and are not considered as digital property as such, but are subject to other regulations. Different individual forms of digital property are usually classified into one of four basic types of these assets: 1) payment tokens (cryptocurrencies) – which represent a means of payment such as cash or electronic money, although in practice they are often used for investment purposes as well (in tokens for payment also includes certain types of stable digital assets); 2) investment tokens – which grant rights similar to the rights associated with the business operations of companies (eg the right to dividends, the right to vote, etc.); 3) user tokens – which give the right to use goods or provide services within a predetermined closed system; 4) hybrid tokens – which have features of two or more of the aforementioned tokens, serve different purposes, and the purposes often change during their existence (European Commission – Commission staff working document, 2018).

The development of digital technology had a dominant influence on the emergence and need for legislative regulation of new institutes in law. The Digital Property Act determines not only the general concept of digital property, but also an indirect classification of digital property in terms of what can be subsumed under the concept of digital property. This is necessary, since innovative solutions in the domain of this field far exceed the possibility of legislative solutions, which will incorporate different possible forms of its appearance in practice within the very concept of digital property. The legislator decided to define two forms of digital property separately, digital token and virtual currency. A digital token is a type of digital property and is defined as any intangible property right that represents one or more other property rights in digital form, which may include the right of the user of the

digital token to be provided with certain services (Digital Property Act, 2020). In terms of the Act, two forms of property are specifically defined under the term digital property, virtual currency and digital token. It is important to point out that this classification of digital property is not limited in scope, and that digital property can also be outside the given classification in accordance with the general definition of the concept of digital property. These two forms of digital property have in practice proven to be particularly important forms of a new type of property whose manifestation in reality is such that their special definition is necessary. What they have in common is that both virtual currency and digital token represent a type of digital property.

The scope of rights arising from the legislative definition of digital property appeares to be complete. The holder of digital property rights can be a natural or legal person. Since the legislator does not expressly limit state subjects as possible holders of rights, an adequate interpretation in the given context is that state entities can be holders of rights arising from digital property, including virtual currencies, or digital tokens. However, the Act stipulates that certain financial institutions, regardless of their legal subjectivity from the aspect of ownership, have limitations in the domain of the right to be holders of digital property. Namely, financial institutions under the supervision of the National Bank of Serbia cannot have digital assets in their assets, nor instruments related to digital property, nor can investments in the capital of those institutions be in digital property (Digital Property Act, 2020).

When it comes to the scope of application of the digital property as legal institute, its limitationsare related to financial instruments. Namely, the way in which digital property is treated legislatively shows a number of legislative similarities in relation to financial instruments. Financial instruments are contracts or any document that acts as a financial asset such as debentures and bonds, receivables, cash deposits, bank balances, swaps, futures, shares, bills, futures, FRA or forward agreement etc. (Vunjak & Kovačević, 2000). Since the method of issuing digital property has a number of legislative similarities with the issuance of financial instruments, the scope of application of the law in the given context addresses this issue in such a way that the issuance of digital propertyhas all the characteristics of a financial instrument, as well as secondary trading and provision of services related to such digital property, the law regulating the capital market applies. The scope of application in the context of the ability to pay is unquestionable. Since digital assets are disposed of like any other form of assets, all payments, collections and transfers in domestic currency in connection with transactions with digital assets are

carried out in accordance with the regulations governing payment services, i.e. foreign exchange operations. In this way, in fact, the legal disposal of all types of transactions in domestic and foreign currency is made possible in accordance with the provisions of the Law on Payment Transactions, that is, the Law on Foreign Exchange Operations.

4. Initial offer of digital property issuance – legal regime of digital property issuance

Digital Property is legislatively innovative institute in national law, which as such has not yet been established in the legal systems of European countries. There are several reasons for this, but certainly one of the most significant is the complexity of the matter itself that is being regulated, dynamic changes in the digital environment that affect the appearance of new forms of digital records that have a property character, as well as the intention of the state to leave matters in this domain with the already existing regulations. The Digital Property Act is conceived as a regulation that, on the one hand, clearly defines the primary institutes in the field of legislative regulation, but also significantly relies on some already existing solutions of the national legal system. A significant part of this regulation addresses the issue of issuing digital property. The very term "issuance of digital property" is largely associated with the act of issuing securities or financial instruments. In the absence of more adequate terms, the legislator uses the term "issuance of digital property", as soon as the institute of digital property is unambiguously connected with financial instruments, i.e. securities. The procedure for issuing digital property is a procedure that basically addresses how a technologically created digital record of a property character appears in legal transactions. Since the legislator clearly defines the term and types of digital property, it is adequate to also regulate how and in what manner digital property appears in the legal context as an object of purchase, sale, exchange or transfer. The scope of application of the Act is within the legal system of the Republic of Serbia, which means that only those digital assets that were created/created within the legal space of the State can be the subject of the offer. The initial offer of digital property issued in the Republic of Serbia is exclusively regulated by the provisions of this Act, including the advertising of digital property. The procedure for issuing digital property is a legally regulated procedure that can be carried out in two ways, advertising the initial offer of digital property for which no white paper has been approved, or advertising digital property for which a white paper has been approved. There are many similarities between

the procedure for issuing financial instruments and the procedure for issuing digital property. The digital property market has certain similarities with the capital market, and certain forms of digital property have features of financial instruments in terms of capital market regulations, i.e. electronic money in terms of payment services regulations (Mihajlović, 2021).

Digital property can be purchased on the primary and secondary markets. The legal regime of the issuance of digital property refers to the appearance of digital property as an object of trading on the primary market. We are talking about relatively similar legal solutions that govern the procedure for issuing financial instruments in accordance with the provisions of the Capital Market Act. Basically, it can be stated that the entire process of issuing digital property represents a relatively identical legislative solution of the aforementioned regulation, the Capital Market Act. The distinctions that appear are a consequence of subject-specific features of digital property. Since digital property represents a new property law institute, the legal regime of the creation of property is of a legal-hybrid character, which is legally identified with the issuance of financial instruments. As a form of property of a digital record, the way digital property appears in legal transactions is related to the way it was created. Taking into account that digital property is created as a consequence of a process based on the application of ICT, which creates a digital record, the legislator decided that the legal moment of the creation of digital property as a legal institute should be regulated through the process of its issuance in a very similar way as prescribed in of the Capital Market Act. Indirectly, the legislator in this way points to the high degree of similarity that exists between digital property on the one hand, and financial instruments on the other.

The very terminology used by the legislator, "issuance" of digital property, is perhaps linguistically questionable. Certainly, the creation of digital property itself is to a large extent "legally innovative", which certainly makes it difficult to standardize this institute. The use of the term "issuance" is not the most precise term, considering the fact that digital propetyis created. Regarding the legal subjectivity of the issuer of digital property, a very liberal solution of the legislator is identified. A domestic or foreign natural person, legal entity and entrepreneur can act as the issuer of digital property (Digital Property Act, 2020). Realizing that digital property arises as a specific property law institute, in the role of issuer of digital property, the legislator determines persons or entities in the most liberal way. Natural and legal entities can be issuers of digital property, but the entrepreneur also appears. The given solution is legislatively interesting and calls into question

why the legislator mentioned entrepreneurs so explicitly, since these persons are primarily natural persons, and only subsequently individual business entities. Their legal status as entrepreneurs is in accordance with the Business Companies Act, but according to that regulation, all entities that register as entrepreneurs are natural persons.

A digital propertyissuer may choose to advertise a digital property. It must be done in accordance with the law, where it is specified that such a procedure can be initiated depending on the fact whether the advertising of the initial offer of digital property is with an approved white paper or without a given document. The legislator primarily focuses on the legislative elaboration of the offer of digital property for which the white paper was approved.

The common denominator is essentially the document that appears during issuance. In the case of financial instruments, it is a prospectus[1], while in the case of issuing digital property, it is a white paper. A white paper is a document published during the issuance of digital property in accordance with this law, which contains information about the issuer of digital property, digital property itself and risks associated with digital property, and which enables investors to make an informed investment decision (Digital Assets Act, 2020). The white paper is the most important document on the basis of which the consumer makes an investment decision regarding a specific form of digital property. Its content should eliminate the risks that consumers face when making that decision, but also familiarize them with the basic features of digital property and its issuer (Mihajlović, 2021). If we analyze what the prospectus or white paper contains, the conclusion that emerges is that the legislator has largely incorporated legislative solutions in terms of the content and method of issuing digital propertythrough a white paper in the same way as it was done with the prospectus, which is an institute of the Capital Market Act and relates to on financial instruments and the obligations of the issuer thereof in connection with the provision of relevant information during the process of issuing securities, i.e. financial instruments that appear on the financial market.If the issuer of digital property decides to offer a digital property for which a white paper has been approved, the advertising of the initial offer refers to advertisements in connection with a specific initial offer of digital property, the aim of which is to promote the purchase of digital

[1] The basic prospectus is a prospectus that contains all significant information from the provisions of Art. 15, 16, 17 and 18 of this law, as well as Article 33 on the issuer and the securities for which a public offer will be made or which will be included in trading, and, if the issuer so decides, may also contain final conditions of the offer. See more: Article 2, point 14. Capital Market Law ("Official Gazette of RS, No. 129/2021)

property, i.e. investment in that asset (Digital Property Act, 2020). It is important to emphasize that the law additionally affirms the legal circulation of digital property, since it clearly determines that it can be bought, that is, that it can be invested in, which represents an identical legal construction that is legislatively recorded within the Capital Market Act. The issuer is obliged to ensure that the white paper contains all information about the issuer and the initial offer that allows buyers/investors to make an informed decision related to the purchase/investment in digital property and understand the risks related to the initial offer and the digital property being offered (Digital Property Act, 2020). The text of the advertisement should clearly indicate that it is in fact an advertisement. The information contained in the advertisement must not be incorrect or misleading, and must be consistent with the information in the white paper, if the white paper has already been published, or with the information to be provided in the white paper, if the white paper will be published. When advertising, the issuer is obliged to state that the white paper has been published or will be published along with information on where and how investors can obtain it. The supervisory authority supervises the issuer's activities related to advertising, and all types of advertisements must be published on the issuer's internet presentation no later than on the same day that the advertisement is published.

5. Conclusion

Until the adoption of the regulation on digital property in the Republic of Serbia, this form of property existed in the intermediate space of regulations that regulated property and financial legal relations. The standardization of digital property continues the process of legal regulation of the digital society in the Republic of Serbia, which benefits both the state itself, society and the economy, as well as business entities and investors. Digital property mainly appeares in the domain of the capital market, which is confirmed by the way of regulation in the Digital Assets Act, as well as the terminology used, which is similar to financial terminology. Today we can talk about the market of virtual or digital property. Seen from the perspective of property law relations, two basic forms of digital property – virtual currency, although used as a means of payment, does not have the status of money or currency, while digital token represents an intangible property right as an emanation of property rights in digital form. In practice, a virtual currency cannot be included as such as a stake in a company, while a token can. In this sense, digital property shows the outlines of a legal institute *sui generis*, with a very strong potential to

influence and redefine property and financial legal rules. Further application of the legally stipulated, but also new forms of digital property in the context of tax system inevitably conditions the issues of its tax treatment, which further creates the need to adapt tax regulations and procedures to the new reality and challenges. It is very certain that the courts will play a significant role in creating the prerequisites for the effective implementation of regulations that regulate both digital property and the usage of digital technology in general. Every new regulation needs to pass the test of time and application, which in this case, as with all regulations that try to standardize the use of digital technology, is a big challenge, because the legislator and the development of digital technology, as well as the modalities of its application, do not move at the same speed , and very often not in the same direction.

Mirković Predrag
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

DIGITALNA IMOVINA – LEGISLATIVNI PRISTUP REGULISANJU NOVOG IMOVINSKOPRAVNOG INSTITUTA

REZIME: Razvoj digitalne tehnologije transformisao je način na koji pojedinac, društvena grupa ili zajednica odnosno država obavljaju interakcije u svojim interesnim domenima. Primena digitalne tehnologije, naročito IKT jeste uslovila potrebu za preispitivanjem da li postojeća legislativna rešenja odgovoraju takvim novinama, ili je nužno pravni sistem države menjati ili dopunjavati novim propisima. Jedno od takvih pitanja jeste kreiranja nove vrste imovine koja se identifikuje kao digitalna imovina ili imovina zasnovana kao kreacija digitalne tehnologije. Predmet istraživanja rada jeste pitanje analiza instituta digitalne imovine sa posebnim osvrtom na legislativni domen načina izdavanja digitalne imovine. Autor je radom afirmisao pitanje značaja legislativnog izazova u normiranju relevantnih društvenih pojava i odnosa u doba intenzivnog razvoja i primene digitalne tehnologije. Cilj rada jeste ostvaren u domenu sprovedene normativne analize relevantnih odredbi Zakona o digitalnoj

imovini u delu koji se odnosi na legislativan pristup normiranju pojma instituta digitalne imovine, kao i partikularnih pitanja iz domena izdavanja digitalne imovine.

Ključne reči: *digitalno društvo, digitalna ekonomija, digitalna imovina, digitalni token, izdavanje digitalne imovine.*

References

1. Mihajlović, J.,& Terzić Danilović, I. (2022). Pružaoci usluga povezanih sa virtualnim valutama –pojedini i statusnopravni aspekti [Providers of services related to virtual currencies – individual and legal status aspects]. *Pravo i privreda,60* (1), pp. 138-160
2. Vulić, M. (2022). Teritorijalna primena Zakona o digitalnoj imovini [Territorial application of the Law on Digital Assets] .In: *Zbornik radova sa XXX susreta pravnika u privredi Republike Srbije*[*Proceedings of the XXX meeting of lawyers in the economy of the Republic of Serbia*](pp. 90-107), Zlatibor:Udruženje pravnika Srbije u privredi
3. Trklja, R. (2021). Digital assets – creation and accounting records. *Ekonomski signali: poslovni magazin*,*16*(2), pp. 115-126
4. Afanas′evna, L. (2021).Digital financial assets, cryptocurrency and digital ruble: terminology and legal regulation, In: *Pravo i digitalizacija* [*Law and digitalization*] (pp. 147-148), Niš: Centar za pravna i društvena istraživanja Pravnog fakulteta u Nišu
5. Mihajlović, B. (2021). Digitalna imovina u pravnom sistemu Srbije: osnovne karakteristike [Digital assets in the Serbian legal system: basic characteristics]. In: Soković, S. (ur.),*Usklađivanje pravnog sistema Srbije sa standardima Evropske unije: zbornik radova* [*Harmonization of the legal system of Serbia with the standards of the European Union: collection of papers*] (pp. 595-609), Kragujevac: Pravni fakultet univerziteta u Kragujevcu, Institut za pravne i društvene nauke
6. Mihajlović, B. (2021). Zaštita potrošača na tržištu digitalne imovine [Consumer protection in the digital asset market].In: Bujisić, D. (ur.), *Zbornik radova: XXI vek – vek usluga i uslužnog prava* [*Harmonization of the legal system of Serbia with the standards of the European Union: collection of papers*] (pp. 369-381), Kragujevac:Pravni fakultet Univerziteta u Kragujevcu:Institut za pravnei društvene nauke
7. Jovanić, T. (2021). Kriptovalute kao novi izazov zaštite potrošača [Cryptocurrencies as a new challenge for consumer protection]. In:*Zaštita*

kolektivnih interesa potrošača: zbornik radova [*Protection of collective interests of consumers: collection of paper*s], (pp. 396-427), Beograd: Pravni fakultet Univerziteta Union

8. European Commission, Commission staff working document – impact assessment, Brussels, 2020, Downloaded 2023, January 15 from:https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:
9. European Commission, Commission staff working document – impact assessment; Downloaded 2023, January 15 from: https://op.europa.eu/en/publication-detail/-/publication/48491c8f-59bb-11ec-91ac-01aa75ed71a1
10. Castells, M. (2000). *The rise of the network society (2nd ed.).* Malden: Wiley-Blackwell
11. Stojšić Dabetić, J., & Mirković, P. (2021). The role of digital technology in keeping modern digital society sustainable. In: *International Scientific Forum "Danube – River of Cooperation"*, (pp. 135–147), Beograd:International Scientific Forum "Danube – River of Cooperation"
12. Stojšić Dabetić, J., & Mirković, P. (2022). *Ugovaranje i ugovorno pravo u digitalnom društvu* [*Contracting and contract law in the digital society*]. Novi Sad: Pravni fakultet za privredu i pravosuđe u Novom Sadu
13. Dukić Mijatović, M., & Mirković, P. (2022). Digitalna ekonomija i informaciono društvo – domet i pristup pravne regulacije [Digital economy and information society – scope and approach to legal regulations]. *Ekonomija – teorija i praksa*, *15*(2), pp. 53–70
14. Vunjak, N., & Kovačević, Lj. (2000). Finansijski instrumenti na tržištu kapitala [Financial instruments on the capital market.In: *Poslovna finansije i finansijsko tržište, Zbornik radova: „Računovodstvo i finansije u tranziciji"* [*Business finance and the financial market, Proceedings: "Accounting and finance in transition"*] (pp. 252-264), Teslić:Savez računovođa i revizora Republike Srpske
15. Zakon o digitalnoj imovini [The Law on Digital Property]. *Službeni glasnik RS,* br. 153/20
16. Zakon o tržištu kapitala [Law on Capital Market]. *Službeni glasnik RS,* br. 129/21

Mladenov Marijana[*]
http://orcid.org/0000-0002-4574-5159

UDK: 159.922:004.8(4-672EU)
Original scientific paper
DOI: 10.5937/ptp2300032M
Received: 24.01.2023.
Approved on: 28.02.2023.
Pages: 32–43

HUMAN VS. ARTIFICIAL INTELLIGENCE – EU'S LEGAL RESPONSE

ABSTRACT: Artificial intelligence (AI) has the capacity to improve not only the individual quality of life, but also economic and social welfare. Although the AI systems have many advantages, they also pose significant risks, creating a wide range of moral and legal dilemmas. The European Union has been creating a legal framework for developing, trading, and using AI-driven products, services, and systems to reduce the risks connected with the AI systems and to prevent any possible harm they may cause. The main focus of this paper refers to the analysis of the Proposal for the Artificial Intelligence Act submitted by the European Commission in April 2021. The goal of the article is to move toward a possible resolution to the dilemma of whether the AIA proposal is appropriate for the AI era by addressing the scope of its application, the prohibited AI practices, rules on high-risk AI systems, specific transparency obligations, as well as certain regulatory gaps. The article should be viewed as an initial analysis of the AIA proposal in order to provide a useful framework for the future discussion.

Keywords: *artificial intelligence, the Europan Union, regulatory framework, the Proposal for the Artificial Intelligence Act.*

[*] LLD, Associate professor, Faculty of Law for Commerce and Judiciary in Novi Sad, The University of Business Academy in Novi Sad, Republic of Serbia, e-mail: alavuk@pravni-fakultet.info

1. Introduction

Artificial intelligence (AI) has transformed many industries in recent years and still attracts global headlines (Perucica& Andjelkovic, 2021. p.348). AI has the capacity to improve not only the individual quality of life but also economic and social welfare (Kolarević, 2022, p.111). However, while AI systems have many advantages, they also pose significant risks, creating a wide range of moral and legal dilemmas (Bjelajac& Filipovski, 2021. p.11).

The European Union has been creating a legal framework for developing, trading, and using AI-driven products, services, and systems to reduce the risks connected with AI systems and to prevent any possible harm they may cause.The European Parliament passed a "Resolution on Civil Law Rules on Robotics" on February 16, 2017, which specifically called for legislation on the liability of robots and AI (Resolution on Civil Law Rules on Robotics, 2017). Furthermore, the Commission adopted "Communication on Artificial Intelligence for Europe" on April 25, 2018 (Communication on Artificial Intelligence for Europe, 2018,). With the help of an expert panel, the Commission stated in this communication that it will examine if the national and EU liability frameworks are appropriate in the context of problems posed by AI. Two years later, the Commission published a package consisting of four documents,including the White Paper "On Artificial Intelligence – A European approach to excellence and trust" (Koch, 2020). In April 2021 European Commission moved ahead with the Proposal for the Artificial Intelligence Act (hereinafter: AIA proposal), which will present the main subject of the research in the paper (Proposal for the Artificial Intelligence Act, 2021).

The AIA proposal is the first initiative to horizontally regulate AI on a global level (Bogucki, Engler, Perarnaud & Renda, 2022). It establishes fundamental, cross-industry norms for the creation, exchange, and application of AI-driven systems, products, and services within EU territory. This act aims to formalize the high requirements of the "Ethics guidelines for trustworthy AI(a)", which calls for AI to be technically proficient, ethical, and lawful while safeguarding democratic principles, human rights, and the rule of law (Hickman & Petrin, 2021). In order to meet this aim, the AIA proposal follows a risk-based approach to differentiate between AI systems uses that create the following categories of risks: "an unacceptable risk, a high risk,and a low or minimal risk" (Explanatory Memorandum of the AIA proposal, 2021, p.12).This implies, among other things, that applications using AI that pose an unacceptable risk are prohibited, while AI systems with low risks, can be created and used in compliance withcurrent regulations.

Considering the abovementioned, the goal of the article is to move toward a possible resolution to the dilemma of whether the AIA proposal is appropriate for the AI era by addressing the scope of this act, the prohibited AI practices, rules on high-risk AI systems, specific transparency obligations as well as certain regulatory gaps.

2. The scope of the AIA proposal

The scope of the AIA proposal is defined by the subject matter of the regulation as well as the scope of its application. Concerning the subject matter, Article 1 states thatthe AIA proposal establishes:

(a) "harmonised rules for the placing on the market, the putting into service and the use of artificialintelligence systems ('AI systems') in the Union;
(b) prohibitions of certain artificial intelligence practices;
(c) specific requirements for high-risk AI systems and obligations for operators of such systems;
(d) harmonised transparency rules for AI systems intended to interact with natural persons, emotionrecognition systems and biometric categorisation systems, and AI systems used to generate ormanipulate image, audio or video content;
(e) rules on market monitoring and surveillance" (Proposal for Artificial Intelligence Act, 2021).

According to Article 1, the AIA proposal regulates "AI systems". Along with the issue of how to distinguish between "AI" and "AI systems", theextremely broad conceptual scope of the AIAproposal also looks unclear. The definition of "AI systems" is provided by Article 3(1) of the AIA proposal, which together with Annex I mainly includes any computer program. As a result of such a wide approach, the designers, operators, and users of AI systems may experience different legal uncertainty(Helberger & Diakopoulos, 2022).Undoubtedly, a broad definition of "AI systems" may be reasonable in the context of the AI practices expressly forbidden by Article 5 of the AIA proposal in order to balance the risks that various types of software pose tofundamental human rights. Contrary, when it concerns high-risk AI systems, such a broad definition is too general. The required conditions proposed within Title III of the AIA proposal for these systems are based on the understanding that many fundamental rights are negatively affected by the unique features of machine learning, including transparency, complexity,

reliance on data, and autonomous behaviour (Smuha et al., 2021, p. 11). The wide definition of AI may result in overregulation because these features are either not present or only partially present in simple algorithms (Ebers, Hoch, Rosenkranz, Ruschemeier & Steinrötter, 2021, p. 591).

In regards to the territorial scope, the AIA would apply to public and commercial actors both inside and outside the EU, so long as their AI system is sold on the EU market or has an impact on EU citizens. The AIA wouldapply to three types of companies (or other parties, including public bodies), that use AI systems in different ways: providers, users, and producers of products used in the EU. The first and third categories, give the AIA proposal extraterritorial impact outside of the EU (Greenleaf, 2021, p. 3).By restricting the geographic application of the AIA proposal to the "use" of AI systems within the EU, it is possible that some high-risk AI systems or even forbidden AI systems are developed, sold, or exported from the EU but used outside the EU. Therefore, it seems that this provision has the potential to create various legal and ethical problems for users of AI systems outside the EU (Ebers, Hoch, Rosenkranz, Ruschemeier, & Steinrötter, 2021, p. 591).

3. Prohibited uses of AI

Article 5 of the AIA proposal establishes a list of prohibited AI practices. The list of prohibited practices includes all AI systems whose use is not in accordance with fundamental European values, such as respect for fundamental human rights and freedoms.Four different types of AI are generally included under the list ofAI practices that are prohibitedunder the standards outlined in Article 5 of the AIA proposal.

The first one, "subliminal or manipulative AI practices", is defined as one that has "*a significant potential to manipulate persons through subliminal techniquesbeyond their consciousness*" to materially modify someone'sbehaviour in a way that harms or is likely to negatively affect their physical or psychological well-being or the well-being of another person (Explanatory Memorandum of the AIA proposal, 2021, p.12). Even though the AIA proposal does not define the term "subliminal", this phrase typically describes a perception that is below the level of awareness (Klein, 1966, p. 726). The activity's potential to harm someonephysically or psychologically should be considered a final trigger. The scope of the provision is significantly limited by this requirement(Veale & Borgesius, 2021 p. 99).

The second type of prohibited AI is referring to the AI practices exploiting vulnerabilities of particularly vulnerable groups including children

or persons with disabilitiesto materially influence a person's behaviour in a way that harms or is likely to harm that person or another person's physical or psychological well-being.The main aspect of this provision is vulnerability, which isnot extensively defined but only demonstrated by the examples of particularly vulnerable groups, such as children or individuals with disabilities (Neuwirth, 2022, p. 7).

The thirdcategory of prohibited AI practices, "social scoring systems", includes systems used by "*public authorities or ontheir behalf for the evaluation or classification of the trustworthiness of natural personsover a certain period of time-based on their social behaviour or known or predictedpersonal or personality characteristics*" (Article 5 of the Proposal for the Artificial Intelligence Act, 2021). It seems that by restricting the use of social scoring to public authorities, the AIA proposal ignores the use of such systems by private businesses, especially in high-risk sectors where they may have the potential to indirectly impactfundamental rights.Various infrastructures including delivery, telecommunications, and transportation are under the authority of so-called AI companies (Rahman, 2017). Therefore, the above exclusion can have serious socioeconomic implications for individuals, which imposes the needto make this provision universally applicable.

The use of "real-time remote biometric identification systems in publicly accessible locations" falls under the fourth category of prohibited AI practices with exception of certain law enforcement reasons (Article 5 of the Proposal for the Artificial Intelligence Act, 2021).The Law Enforcement Directive (Directive (EU) 2016/680),regulates the use of biometric identification for law enforcement purposes.The widely accepted critics of the doctrine are referring to the narrow scope and limitation of lawenforcement thatallows the use of such AI systems for different purposes (Gill-Pedro, 2021).The use of remote biometric identification for non-law enforcement objectives like crowd control or public health is not prohibited by the restriction. The GDPR normally applies to these uses (Regulation (EU) 2016/679). In general, the GDPR imposes a criterion of high-quality, individual permission for each person scanned, which is practically hard to provide in the absence of a corresponding Member State law authorizing such biometrics (Veale & Borgesius, 2021, p. 101).

In addition, the fact that Article 5 could not be amended by the European Commission could be quite challenging in the context of the implementation of the AIA due to the fact that some problematic aspects of AI practices can only be recognized ex-post.

4. Rules on high-risk AI systems

For AI systems that create a high risk to human health and safety or fundamental rights, or "high-risk AI systems," Title III of the AIA proposalestablishes a new regulatory regime with precise standards. The AIA Proposal adopts a prescriptive "list-based approach," which outlines which systems are considered a high risk rather than defining the term itself.Based on the AI system's intended use and current product safety regulations, a system is categorized as high-risk. As a result, the categorization of a high-risk depends not only on the task performed by the AI systembut also on the precise objectives and operating procedures of that system.

Two main groups of high-risk AI systems are identified in Title III, along with the classification criteria. Systems intended for use as safety components of products that are covered by "third-party ex-ante conformity assessment" under EU law are included in Annex II of the proposal as high-risk systems, as are other standalone AI systems used in high-risk domains (Explanatory Memorandum of the AIA proposal, 2021, p. 14).The European Commission has identified eight use categories for high-risk standaloneAI systems listed in Annex III. By using a set of criteria and a risk assessment methodology, the European Commission may expand the list of high-risk AI systems used within specified pre-defined sectors in order to ensure that the legislation may be modified to develop uses and applications of AI.However, it is important to note that the Commission can only do this if the high-risk AI systems are intended to be used in any of the activities stated in Annex III points 1 through 8. This provision could be quite challenging due to the fact, that we cannot be aware of all categories of high-risk systems sinceAI is a rapidly evolving field that is progressively influencing other industries (Smuha et al., 2021, p. 11).

In addition, Chapter 2 outlines the legal requirements for high-risk AI systems related to "*data and data governance, documentation and recording keeping, transparency and provision of information to users, human oversight, robustness, accuracy and security*" which links to obligations of regulated actors stated within Chapter 3 (Explanatory Memorandum of the AIA proposal, 2021, p. 13). The great majority of all obligations are theresponsibility of providers.With respect to data and data governance, Article 10 of the AIA proposal mostly refers to training, validation, and testing data sets. Data quality criteria for sets of data on individuals, or groups of people (not necessarily involving personal data in GDPR terms), including "special categories of personal data" (as defined in Article 9 of GDPR) are highly detailed in the subject requirements (Regulation (EU) 2016/679).

The following requirement is referring totechnical documentation. Providers must submit technical documentationthatincludes all information in line with Annex IV. Moreover,according to Article 12 of the AIA proposal and record-keeping requirements, providers need to facilitate logging in order to enable traceability that is acceptable for a system's risks.Providers are only required to keep logs for the relevant period while such logs are still under their control; otherwise, users are required to do so.The standards for high-risk AI systems transparency are defined in Article 13. A high-risk AI system must be created in accordance with Article 13 in order to be "sufficiently transparent to enable users to interpret the system's output and use it appropriately" and it must also come with instructions and information that are "relevant, accessible, and comprehensible to users" (Article 12 of the Proposal for the Artificial Intelligence Act, 2021). In addition to the standards above, Article 14 stipulates that providers must create systems that can be properly supervised by natural persons, using "human-machine interface tools" (Article 14 of the Proposal for the Artificial Intelligence Act, 2021). To ensure the protection of fundamental rights, oversight is necessary for all actions linked to the creation, implementation, and use of AI systems.Moreover, Article 15 states that high-risk AI systems must be created and constructed in such a way that, in the context of their intended use, they achieve the required level of accuracy, robustness, and cybersecurity and operate consistently over the period of their lifecycle (Article 15 of the Proposal for the Artificial Intelligence Act, 2021).

The framework for notified bodies' participation in conformity assessment processes as independent third parties is provided in Chapter 4, while the specific conformity assessment processes that must be implemented for every type of high-risk AI system are included in Chapter 5. The approach to conformity assessment aims to reduce pressure on both notified entities and economic operators, whose capability must be gradually ramped up through time.

5. Specific transparency obligations

Title IV of the AIA proposal outlinesspecific transparency obligations. The AIA proposal introduces transparency requirements for systems thatinteract with humansdue to the fact thatpeople have a right to know when they are engaging with a machine's algorithm rather than a human being. Similar requirements for transparency apply to the disclosure of deep fake/ synthetics, biometric categorization, and automated emotion detection systems.Except for biometric categorization systems that are legally allowed to be used for crime prevention, users of emotion recognition or biometric

categorization systems are required to notify exposed persons of the system's operation. In comparison with data protection law, it is quite challenging to understand the contribution of this provision. Data protection law indicates that users of emotional recognition or biometric categorization systems that process personal datanotify individuals of, among other things, the existence and purposes of such processing.Therefore, it is difficult to determine what is the real scope of this provision.

In addition, specific transparency obligations are also introduced for limited-risk AI systems like chatbots. The Low-Risk AI Systems category is the only one that is excluded from transparency obligations (Kop, 2021).

6. Identifying additional regulatory gaps of the AIA proposal

Even though the above analysis of the AIA proposal has already identified certain aspects of the Act that need further clarification, the doctrine concluded that this act has some additional gaps. The most significant one is referring to the fact that the AIA proposal does not include any individual right of enforcement. Although the Act is designed to protect fundamental rights, it has no remedies through which individuals can seek redress if the regulation is violated. The AIA proposal does not include any mechanism to allow individuals to challenge AI-driven decision-making (Ebers, 2021 p. 19).

Moreover, a European approach to AI, on the other hand, should consider not only human rights but also other priorities such as climate change and sustainability. In this respect, the AIA proposal makes no direct mention of "Green AI" or "Sustainable AI" as a clear objective of a European understanding of AI development according to the standards of the European Green Deal (Gailhofer et al. 2021). The Act only recognizes the necessity for relevant action in the high-impact field of climate change and the potential of AI to help socially and environmentally positive outcomes.

7. Conclusion

The AIA proposal intends to establish a uniform legal system for AI in the EU. Through a comprehensive framework, the AIA proposal addressesboth the potential benefits of AI and the moral questions raised by the different threats associated with it.Nevertheless,some aspectsrequirefurther clarification.The main aspect that needs to be improved is the definition of the term "AI". The AIA proposalincludes a quite broad definition, which increases the risk of overregulation of systems. Furthermore, the lack of individual enforcement

rights in the AIA proposal underminesthe protection of fundamental rights as the most important goal of this regulation. The AIA must guarantee the right to remedy that addresses potential Regulation violations or infringements of fundamental rights.

This article cannot and has not discussed all aspects of the AIA proposal. The author has demonstrated some of the complexities of this particularly significant instrument. After all, creating a safe and adequate regulatory framework for AI in Europe is not only the way we design technology but also the way we shape our society's future.

Mladenov Marijana
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

LJUDSKA PROTIV VEŠTAČKE INTELIGENCIJE – PRAVNI ODGOVOR EU

REZIME: Veštačka inteligencija ima kapacitet da poboljša ne samo kvalitet života pojedinca, već i ekonomsko i socijalno blagostanje. Iako sistemi veštačke inteligencije imaju mnoge prednosti, oni takođe predstavljaju značajne rizike, stvarajući širok spektar moralnih i pravnih dilema. Evropska unija kreira pravni okvir za razvoj, trgovinu i upotrebu proizvoda, usluga isistema vođenih veštačkom inteligencijom kako bi smanjila rizike povezane sa sistemima veštačke inteligencije i sprečila svaku moguću štetu koju oni mogu da izazovu. Glavni fokus ovog rada odnosi se na analizu Predloga Uredbe o veštačkoj inteligenciji koji je Evropska komisija podnela u aprilu 2021. Cilj članka je da pruži doprinos u kontekstu razrešenja dileme da li je predlog navedene uredbe adekvatan zahtevima ere veštačke inteligencije, adresirajući obim primene ovog akta, zabranjene prakse veštačke inteligencije, pravila o visokorizičnim sistemima veštačke inteligencije, specifične obaveze transparentnosti kao i određene pravne praznine. Članak treba posmatrati kao početnu analizu predloga Uredbe o veštačkoj inteligenciji kako bi se obezbedio koristan okvir za buduću diskusiju.

Ključne reči*: veštačka inteligencija, Evropska unija, regulatorni okvir, Predlog Uredbe o veštačkoj inteligenciji.*

References

1. Artificial Intelligence Act. (2021). Proposal for a regulation of the European Parliament and the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. EUR-Lex – 52021PC0206
2. Bjelajac, Ž., &Filipović, A. M. (2021). Specifičnosti digitalnog nasilja i digitalnog kriminala [Specific characteristics of digitaliolence and digital crime]. *Pravo – teorija i praksa*, *38*(4), pp. 16-32. DOI: 10.5937/ptp2104016B
3. Bogucki, A., Engler, A., Perarnaud, C., Renda, A. (2022). The AI Act and Emerging EU Digital Acquis, Overlaps, gaps and inconsistencies, CEPS. Downloaded 2022, September 23 from https://www.ceps.eu/wp-content/uploads/2022/09/CEPS-In-depth-analysis-2022-02_The-AI-Act-and-emerging-EU-digital-acquis.pdf
4. Communication from the Commission to the European Parliament, the European Council, the Council, European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe. (2018). COM(2018) 237 final
5. Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119/89
6. Ebers, M. (2021). Regulating Explainable AI in the European Union. An Overview of the Current Legal Framework. In: Colonna, L., Greenstein G. (eds.), *Nordic Yearbook of Law and Informatics*, (pp. 1-20). Downloaded 2022, October 15 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3901732
7. Ebers, M., Hoch, V. R., Rosenkranz, F., Ruschemeier, H., & Steinrötter, B. (2021). The European commission's proposal for an artificial intelligence act – a critical assessment by members of the robotics and AI law society (RAILS). *J – Multidisciplinary Scientific Journal*, *4*(4), 589-603. DOI: 10.3390/j4040043
8. European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. (2017). (2015/2103(INL))

9. Gailhofer, P., Herold, A., Schemmel, J.P., Scherf, C.-S., Urrutia, C., Köhler, A., &Braungardt, S. (2021). *The Role of Artificial Intelligence in the European Green Deal, Study Requested by the AIDA Committee of the European Parliament, Study requested by the AIDA Committee*. Downloaded 2022, October 15 from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662906/IPOL_STU(2021)662906_EN.pdf
10. Gill-Pedro, E. (2021). The Most Important Legislation Facing Humanity? The Proposed EURegulation on Artificial Intelligence. *Nordic Journal of European Law,4*(1), pp. 4-10. Downloaded 2022, October 5 from https://journals.lub.lu.se/njel/article/view/23473/20819
11. Greenleaf, G. (2021). The 'Brussels effect' of the EU's 'AI Act'on data privacy outside Europe. *Privacy Laws & Business International Report,* 1, pp. 1-10. Downloaded 2022, September 25 from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3898904
12. Helberger, N., & Diakopoulos, N. (2022). The European AI act and how it matters for research into AI in media and journalism. *Digital Journalism*, pp. 1-10. DOI: 10.1080/21670811.2022.2082505
13. Hickman, E., Petrin, M. (2021). Trustworthy AI and Corporate Governance: The EU's Ethics Guidelines for Trustworthy Artificial Intelligence from a Company Law Perspective. *Eur Bus Org Law Rev*, 22, pp. 593–625. DOI: 10.1007/s40804-021-00224-0
14. Klein, E. (1966). *A Comprehensive Etymological Dictionary of the English Language*. Amsterdam:Elsevier
15. Koch, B. A. (2020). Liability for Emerging Digital Technologies: An Overview. *Journal of European Tort Law*, *11*(2), pp. 115-136. DOI: 10.1515/jetl-2020-0137
16. Kolarević, E. (2022). Uticaj vještačke inteligencije na uživanje prava na slobodu izražavanja. [The influence of Artificial intelligence on the right to freedom of expression] *Pravo – teorija i praksa, 39*(1), pp. 111-126. DOI: 10.5937/ptp2201111K
17. Kop, M. (2021). EU Artificial Intelligence Act: The European Approach to AI. *Transatlantic Antitrust and IPR Developments*, 2, 1-11. Downloaded 2022, October 15 from https://law.stanford.edu/publications/eu-artificial-intelligence-act-the-european-approach-to-ai/
18. Neuwirth, R., J. (2022). *Prohibited Artificial Intelligence Practices in the Proposed EU Artificial Intelligence Act*. DOI: 10.2139/ssrn.4261569
19. Perucica, N., Andjelkovic, K. (2022). Is the future of AI sustainable? A case study of the European Union. *Transforming Government: People, Process and Policy*, *16* (3), pp. 347-358. DOI: 10.1108/TG-06-2021-0106

20. Rahman, K. S. (2017). The new utilities: Private power, social infrastructure, and the revival of the public utility concept. *Cardozo L. Rev*., 39, 1621-1692. Downloaded 2022, October 5 from https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1987&context=faculty.
21. 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 119/1
22. Smuha, N. A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R., & Yeung, K. (2021). *How the EU can achieve legally trustworthy AI: a response to the European commission's proposal for an artificial intelligence act*. DOI: 10.2139/ssrn.3899991
23. Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act—Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, *22*(4), pp. 97-112. DOI: 10.9785/cri-2021-220402

Golić Darko[*]
https://orcid.org/0000-0003-2315-5040

UDK: 342.9:004.738.5(497.11)
Review article
DOI: 10.5937/ptp2300044G
Received: 13.01.2023.
Approved on: 24.02.2023.
Pages: 44–62

NORMATIVE REGULATION OF ELECTRONIC ADMINISTRATION IN REPUBLIC OF SERBIA

ABSTRACT: Following the general trend of the technical-technological progress in society, where technology is increasingly important in everyday life, states and public authorities on all continents strive to facilitate the exercise and protection of the rights of their citizens, and to remove bureaucratic barriers that previously existed and were a common accompaniment appearance of the administrative procedure. As an expression of such an aspiration, but also as a necessary consequence of the technical progress, many countries are introducing a system of electronic public administration. Following this trend, our legislator also establishes a system of electronic public administration, with which he tries to facilitate the exercise of citizens' rights, but also to improve the image that citizens have of a public administration, previously known for its sluggishness and inefficiency. The introduction of electronic administration into the domestic legal system, on the other hand, was done without a sufficient preparation, and it was not realized without certain difficulties, both at the normative level as well as at the level of the implementation of various normative solutions. This paper presents the legal regulations, i.e. the normative framework regulating the introduction and functioning of electronic administration in Republic of Serbia.

[*] LLM, Associate professor at the Faculty of Law for Commerce and Judiciary in Novi Sad, University of Business academy, Novi Sad, Republic of Serbia, e-mail: g.darko83@gmail.com

Keywords: *electronic administration, administrative procedure, the Electronic Administration Act.*

1. Introductory remarks

As a consequence of the development of society and technology, and the overall civilizational progress, modern society[1], especially at the national levels, is characterized by an exceptional dynamic of overall social, economic, legal, economic, sociological, political and other processes and relationships, which also conditions a stronger connection between public authorities and subjects under its jurisdiction. This connection of the public authority with those under its jurisdiction – individuals, legal entities, business entities, etc. – is achieved through modern technology, and especially through the use of various electronic services, with the special aim of achieving the principles of efficiency and economy – timely and high – quality services with the least expenditure of time and material resources (Vučinić, 2020, p. 45).

Thus, the Government of the Republic of Serbia designates e-government as the use of information and communication technologies (ICT), which provide opportunities for citizens and businesses to communicate and cooperate in business with the public administration, using electronic media (Internet, mobile phone, smart cards, etc.) (Đurašković, 2016, p. 17).

As the concept of E-government, at least from the aspect of legal regulation of this social technical-technological project, is relatively new in the this area, legal regulation is still in the development stages, and represents an extremely dynamic component of domestic legislation, where special importance is put on theby-laws. Thus, bearing in mind the fact that the concept of E-government is a new phenomenon in our region, this concept is not even mentioned in the Constitution of the Republic of Serbia, as the highest act of our legal order. In this sense, it can only be stated that, when it comes to the Constitution of the Republic of Serbia, the same framework that applies to public administration is applied to electronic administration.

[1] In practice of comparative countries we find an example of introduction of electronic system in public governmentway back in 1997, when Australia introduced special informational system in the social security sector. To help in task executions, "Centerlink" system was introduced, as unique electronica administrative place (one counter for forehead administration in the socialsecurity sector). In more detail see: Henman, 2010, p. 51.

The legal norms governing electronic administration in the Republic of Serbia are currently found in various positive legal regulations. In addition to individual norms on the introduction of information and communication technologies in connection with the general administrative procedure contained in the "new" Law on General Administrative Procedure (LGAP), in Serbia there is also a special law dedicated exclusively to electronic administration issues – the Electronic Administration Act (EAA). In addition to these laws, various forms of digital behaviour and use of information and communication technologies are found in laws that regulate special (administrative) areas. This, therefore, means that practically the entire regulation of electronic administration in the Republic of Serbia is found in various acts, while a certain part of the regulation is certainly found in by-laws, which appear as a logical and necessary consequence of the fact that the system of electronic administration in Serbia continues to develop, and quick and simple adjustments are often necessary to eliminate the problems that have arisen, or due to the expansion of the range of services offered to citizens and the economy.

Here is an overview of the regulations that govern electronic administration in the Republic of Serbia, starting with the Electronic Administration Act, as a systemic law, and other laws and by-laws.

2. Electronic administration act – systemic law in the regulation of electronic administration in the Republic of Serbia -

The exceptional importance of electronic administration for the Republic of Serbia is also evidenced by the special legislation contained in the Law on Electronic Administration, as a systemic law governing this area.

The initial article of this Act stipulates that this law regulates "the administration of state bodies and organizations, bodies and organizations of provincial autonomy, bodies and organizations of local self-government units, institutions, public companies, special bodies through which regulatory functions and legal and natural persons who are entrusted with public powers (hereinafter referred to as the authority) using information and communication technologies, i.e. the conditions for establishing, maintaining and using interoperable information and communication technologies of the authority (hereinafter: electronic administration)." Paragraph 2 of the same article provides that "The provisions of this law shall accordingly be applied to

other affairs of state bodies when they act in electronic form, unless otherwise regulated by another law" (Article 1 EAA).[2]

Generally speaking, therefore, the Electronic Administration Act seeks to comprehensively[3]regulate the use of information and communication technologies and electronic communication, as well as the exchange of data between various public administration bodies, on the one hand, and citizens and business entities, on the other hand. Although the various elements of electronic administration are contained in special regulations, the Electronic Administration Act states that the issues of electronic administration regulated by that law cannot be regulated or changed by special laws, and everything, we believe, is for the purpose of uniform electronic handling of public administration bodies, as well as equal protection of rights and positions of citizens and other subjects.

When we talk about the application of this Law, Article 2 establishes the widest, almost absolute,[4]application of this regulation to the electronic communication of public administration bodies when they perform not only administrative activities, but also when they perform other tasks of state bodies, either in relation to other bodies or to the citizens. Thus, Article 2

[2] It is interesting to point out that, despite the fact that this law is the so-called "systemic law" when it comes to the regulation of electronic administration in the Republic of Serbia, paragraph 2 of article 1 of this law gives priority to the provisions of special laws in relation to the provisions of this law – this follows from the words *"...if not otherwise regulated by another law."* Starting from the concept of "systemic law", as a creation of our Constitutional Court, no matter how legally logical it may be, it is not usual for "systemic law" to give priority to a special law. On the contrary. The Constitutional Court coined the concept of a "systemic law" precisely in order to give priority to a law that comprehensively regulates one area over other laws, that is, to create something like a "supra-law ". However, Article 3 of EAA provides that "issues of electronic administration, which are regulated by this law, cannot be regulated differently by a separate law, except in the cases provided for by this law." These provisions of Article 1, Paragraph 2 and Article 3 of the Law are contradictory to each other. However, we believe that such a somewhat clumsy provision should be understood as meaning that it is necessary to comprehensively harmonize acts and by-law regulations in order for the mentioned provision to come to life in practice. This is of particular importance in order to ensure the standardization that is necessary for the high-quality functioning of electronic administration and the corresponding uniform degree of protection of citizens and other subjects.

[3] Although the EAA has a total of 55 articles, it can be said that this law regulates all the basics of electronic administration, as well as all key issues of electronic administration in our country.

[4] Only exceptionally, the electronic administrative action of the authorities in accordance with this law does not include the action with acts which, in accordance with the law regulating data confidentiality, are designated as secret and marked with a certain degree of secrecy (Article 2, paragraph 3 of the EAA). Therefore, dealing with classified acts is the only one to which the provisions of this law will not be applied, when it comes to electronic communication by public administration bodies.

of the Law, as a general norm in electronic administrative procedures, prescribes "The authority is obliged to perform electronic administrative procedures and communicate electronically in accordance with this law and the regulations adopted on its basis." In addition, paragraph 2 stipulates that the provisions of this law shall be applied "and on electronic communication between authorities, as well as on the communication of those authorities with parties in the performance of tasks within the scope and competence of state authorities that do not relate to administrative proceedings, unless otherwise regulated by a special law." This kind of regulation, therefore, foresees the full application of this law to the overall electronic communication and actions of public administration bodies.

The next thing that the legislator paid attention to, in systematizing the legal provisions, are the basic principles that are included in the provisions of articles 5-7 of the Electronic Administration Act. According to these provisions, the basic principles on which electronic administration is based in our country are: the principle of efficiency of equipment management, the principle of security of electronic administration and the prohibition of discrimination (see in detail Palević, 2020, p. 529). These, conditionally speaking, "special" basic principles of electronic administration do not exclude the application of general constitutional principles and general principles of administrative procedure in the use and application of information and communication technologies by public administration bodies.

The principle of efficiency of equipment management, as the first of the special principles of electronic administration, is provided for in Article 5 of the Law according to which "The Authority is obliged to efficiently manage the equipment at its disposal so as to enable its proper and economical use." This principle implies that the authority must ensure efficient and economical application of information and communication technologies in accordance with technical rules and rules of general and special administrative procedures, whichever are applied in the specific case. From the legal language – "proper ... use" of technology – it follows that technologies must not be used contrary to the purpose for which they were introduced into the public administration system, which is, in the first place, the satisfaction of the public interest and needs of citizens, as well as others subjects.

The principle of security of electronic administration, prescribed by Article 6 of the EAA, implies that "information systems, electronic communication networks and equipment used to perform electronic administrative procedures must meet the conditions and standards of information security, in accordance with the regulations." One could, however, criticize the approach of the

legislator to completely prescribe the obligation of compliance "with the regulations" – which includes both law's and by-law regulations related to information security. We believe that, although it is a principle that, like any principle, should remain at a general and abstract level, the legislator could and had to prescribe somewhat narrower and stricter conditions that public administration bodies must, as a minimum, respect in terms of information security, and all in order to protect the interests and rights of citizens and other entities that, in some way, form part of electronic administration.[5]

Finally, as a particularly highlighted (similarly Palević, 2020, p. 532) principle of electronic (public) administration, prescribed by Article 7 of the EAA, is the principle of prohibition of discrimination, which, as a general principle of modern societies, is contained in the Constitution and found its place in sphere of electronic administration. It refers to two moments. First, all persons have the right to use the services of electronic services and electronic administrative procedures, which means that everyone must be able to have electronic access to the public services offered, regardless of any personal characteristics. Second, persons who are unable (for example, persons with disabilities) to use electronic administration services in their original form, must be enabled to use the services adequately to the circumstances of the specific case and in accordance with their capabilities. The EAA does not say anything about the concretization of this principle, the setting of limitations or conditions, and it is left to regulations of lower legal force and practice to regulate the content of this principle more precisely.

The entire next chapter of the EAA is dedicated to infrastructure in electronic administration. This – the second – chapter is the most extensive chapter of the Electronic Administration Act, which, in its provisions of Articles 8-31, contains substantial norms that establish and regulate the system of electronic administration, its elements and the manner of its functioning, and includes a significant number of provisions related to the technical aspects of the electronic administration system: 1) Unified information and communication network of electronic administration; 2) Service bus of the organ; 3) Establishment and management of registers and records in electronic form; 4) Use of data from registers and records in electronic form; 5) Protection of data and documents during their acquisition and transfer; 6) Establishment and management of Metaregistry; 7) Unique

[5] Nevertheless, it should be emphasized at this point that the legislator did pass the Law on Information Security which regulated many issues in the domain of information security, and this law represents a part of the broader system of electronic administration in the Republic of Serbia.

electronic mailbox; 8) Software solution; 9) e-Administration portal; 10) Work of authorities on the e-Administration Portal; 11) Authorized persons of the e-Administration Portal; 12) Obligations of the main administrator of the e-Administration Portal; 13) Obligations of body administrators on the e-Administration Portal; 14) Rights of users of electronic administration services on the e-Administration Portal; 15) Establishing and maintaining a web portal in electronic administration; 16) Reuse; 17) Licenses for reuse; 18) Open data portal; 19) Creating and maintaining a web presentation; 20) Physical protection of data and storage of backup copies; 21) Maintenance, repair and decommissioning of work equipment; 22) Conditions for establishing electronic administration. Within this part, a separate article establishes the conditions for the establishment of electronic administration (a total of 20 conditions are prescribed).

The third chapter of the EAA is dedicated to electronic administrative procedure, which essentially has two parts of provisions. The first part refers to the establishment and connection of an individual body to the electronic administration system, which includes provisions on the establishment of electronic administrative procedures of the body, conditions for obtaining and transferring data and electronic documents, user authentication, user authorization and identity federation.[6] The second part of this chapter refers only to practical electronic administrative procedures of public administration bodies. Thus, the provisions of Articles 37–42 of the EAA the obligations of authorities in communication with the user of the electronic administration service,[7]electronic submission, receipt of electronic submission, electronic delivery, confirmation of electronic delivery, as well as the e-mail address of

[6] Articles 32–36 of the Law on Electronic Administration; Article 36 talks about the Federation of Identity. This choice of terminology is very interesting, bearing in mind the generally accepted and usual meaning of the word "federation". However, in the EAA, the legislator opted for the use of a new strictly professional terminology. In this sense, the identity federation means "a set of Identity Providers, Service Providers and Federation Operators who, under agreed conditions, cooperate in order to authenticate and exchange appropriate data about end users in order to enable them to use the service." Glossary of terms of the Academic Network of Serbia, available at https://www.amres.ac.rs/cp/institucije/iamres-federacija-identiteta/recnik-pojmova.

[7] Although this provision could be subsumed under the first part of this chapter, which refers to the establishment and connection to the electronic administration system, it was still considered to belong to the second part. This is because this provision stipulates the authority's duty to publish on its web presentation, eAdministration Portal and/or other web portal a list of administrative procedures that can be carried out electronically, as well as the way of conducting electronic administrative procedures and restrictions on electronic administrative procedures (Article 37 EAA). As this notification refers to practical electronic administrative procedures, we classified this provision in the second group of chapter III of the law.

the authority in electronic administrative proceedings are prescribed. So, as we can see, the second part is dedicated to the arrangement and verification of electronic communication between public administration bodies and citizens, as well as the submission of various certificates issued by the administration bodies.

The last three chapters are, as usual, dedicated to supervision, penal provisions and transitional and final provisions. Thus, the provisions of Article 43 of the EAA stipulate that the supervision of the implementation of this law and the regulations adopted on the basis of it shall be carried out by the ministry responsible for the development of electronic administration. Penal provisions provide for a misdemeanour on the responsibility of the main administrator of the web portal, the administrator of the body on the web portal, the responsible person in the body authorized to keep electronic registers and the responsible person in the body if they act contrary to certain provisions of the law. Transitional and final provisions prescribe deadlines for: adoption of by-laws (six months from the date of entry into force of this law); establishment of the Service Bus of authorities for the exchange of data from registers; establishment of registers and records in electronic form; establishment of Metaregistry ; development of software solutions; electronic administrative procedure; transfer of e-mail registers and orders to servers in the Republic of Serbia; as well as the provisions on the entry into force of the law.

It is clear from the above that the Electronic Administration Act, although it is not one of the most comprehensive legal texts, regulates the key and basic issues of electronic administration in the Republic of Serbia in a fairly comprehensive manner. True, as it was pointed out, the legislator left the regulation of a significant part of the matter to the executive and administrative authorities, which will regulate numerous issues with by-laws, thus creating a coherent and unified set of regulations on electronic administration. Although the legislator's decision to leave the prescription to the executive and administrative authorities should always be approached with scepticism and with a degree of caution, we believe that leaving the law to the executive branch, in the case of electronic administration, was necessary and justified, bearing in mind the trend of constant and rapid technical-technological progress. In addition, it is quite reasonable to expect that during the establishment and expansion of the electronic administration system, there will be necessary interventions regarding the regulation of certain issues. Bearing in mind the complexity and time period necessary for the adoption of the law, as well as its amendments and additions, in the case

of electronic administration, leaving a significant part of the prescription of provisions to the executive and administrative authorities, our legislator was wise.

3. Other laws regulating certain issues of electronic administration

Despite the fact that there is a special law regulating the field of electronic public administration, not all aspects and all relevant issues of electronic administration in the Republic of Serbia are regulated by the Electronic Administration Act, as a systemic law, nor would it be possible by the nature of things. On the contrary, other legal regulations regulating both general and special administrative procedures contain some special rules related to electronic administration, in relation to electronic administrative procedures.

a) Law on General Administrative Procedure

The Law on General Administrative Procedure is also important for the electronic actions of administrative bodies. Namely, the LGAP comprehensively regulates the rules of the general administrative procedure, which initially, for the first time, established the legal basis for electronic proceedings, which was further elaborated by the adoption of the Electronic Administration Act (Milkov, 2017, p. 133 et seq.).[8]This primarily refers to the possibility of public administration bodies to teach applicants, receive requests for recognition of rights or other types of submissions in administrative matters and to inform the applicant about the progress of the procedure electronically (LGAP, Article 12). As an example of the introduction of digitization of work in the work of administrative bodies, the obligation of the body to ex officio acquire and process data on the facts of which official records are kept, and which are necessary for decision-making, is often highlighted.[9]Authorities can also exchange such data electronically (LGAP, Article 103). This way of acting, essentially, stands in a strong connection with the principles of effectiveness and economy, but also with the final provisions, where it is foreseen that the provisions of special laws that require the parties to submit

[8] At the same time, one must not lose sight of the fact that the LGAP was adopted in 2016, while the EAA was adopted in 2018.

[9] However, practice shows that public administration bodies are still not fully prepared to do this ex officio, and the party still has to obtain the necessary documents on its own.

documents that prove the facts of which the authorities keep official records will cease to be valid (see LGAP, Article 215). Storing databases and various documents in electronic form also enables viewing of case files in digital form. One of the most important actions in the administrative procedure is service(delivery), which, although it is a form of informing the participants of the procedure, has a great impact on the rights, obligations and interests of the parties. All forms of delivery (personal and indirect) can also be done electronically, provided that the parties have agreed to it. The delivery note, as a confirmation that personal or indirect delivery has been made, can be in electronic form (LGAP, Article 72 and 77). Also, there are no legal obstacles to the fact that the decision, as the most important act in the administrative procedure for the adoption of which the administrative procedure is initiated, and which resolves the administrative matter that ends the administrative procedure, can be issued in the form of an electronic document.

In addition to the above, in the general administrative procedure there is room for the introduction of additional digital elements, which also refers to the way the entire procedure is conducted, the performance of evidentiary actions and the adoption of an administrative act. While it is true that LGAP recognizes the institute of video-conference oral hearings, but only for those bodies that have the technical capabilities to schedule and hold such type of hearings (LGAP, Article 111). This way of holding discussions digitally must be gradually introduced as a rule, and not, as is the case in practice, as a rarely used exception.

Certainly, with the increasing digitization of the general administrative procedure, space is opened for the introduction of more digital elements in special administrative procedures as well.

b) Law on tax procedure and tax administration

The provisions of the Law on General Administrative Procedure and the Electronic Administration Act are generally followed by laws governing special administrative areas. Such is the case with the Law on Tax Procedure and Tax Administration (hereinafter: LTPTA). LTPTA certainly takes into account the fact that citizens and business entities have long since switched to electronic means of communication and digital documentation management in their jobs. As a result, when it is necessary to access data important for determining taxes and tax obligations, taxpayers must provide the necessary documents in electronic form on electronic data carriers (LTPTA, Article 37a).

For the stated reason, electronic communication between parties and tax authorities is enabled. Taxpayers are allowed to submit tax returns to the tax authority in electronic form. In a similar way as in the matter of the general administrative procedure, the LTPTA regulates the form of acts issued by the tax authorities in the tax procedure. Thus, Article 35 of the LTPTA stipulates that the tax administrative act, as a special form of administrative act, can be passed in electronic form. The situation is the same with other tax-administrative acts that are passed for the purpose of guiding and making decisions in the tax procedure (Ivanović & Knežević, 2013).

c) Customs Law

Information and communication technology has also found its application in the area of customs procedure, as a special administrative procedure. The considerable amount of information and data that customs authorities have to exchange with other administrative authorities and citizens, as well as with business entities, requires efficient and reliable exchange of large amounts of data and fast communication and distribution thereof. Therefore, the importance of information and communication technologies in the performance of tasks under the jurisdiction of customs administrative bodies is also recognized by the systemic law in this area – the Customs Act. This law regulates the rules and procedures that apply to goods that are imported and exported from the customs territory of the Republic of Serbia. Customs authorities, therefore, according to the express provision of Article 4 of the Customs Law, have the obligation to introduce and apply information and communication technologies, when it is cost-effective and efficient for the Customs Administration, as well as for the economy in general.

Information and communication technologies are understood as methods of electronic trade and methods of electronic determination of the correctness of data and goods. Certain actions can be performed electronically, such as the submission of declaration and summary declaration. In general, customs authorities must enable communication with business entities to take place electronically, which respects the needs of a developed society and a developed economy. It should be especially emphasized that, given that the customs procedure is a special administrative procedure, and that the general rules on the subsidiary application of the rules of the LGAP apply to it, if any of the issues are not specifically regulated by a special – Customs – law, they are subject to apply the norms of the general administrative procedure, which refers to "digital provisions", but also to the provisions of the Electronic Administration Act.

d) Law on State Survey and Cadastre

The Law on State Survey and Cadastre is another special law that governs a special administrative area. The subject of regulation of this law, according to Article 1, are professional jobs and jobs of the state administration related to the state survey, real estate cadastre, water cadastre, address register, etc. For obvious reasons, the cadastre must quickly and efficiently perform tasks within its jurisdiction, since the realization and enjoyment of property rights, as one of the basic human rights, but also the realization of many other rights, depends precisely on the quality functioning of this body. For this reason, Article 119 of the Law prescribes that data on changes to immovable property be requested from the competent authority electronically, and the same shall be submitted to the competent authority in the same way, through the WEB service.

For easier and more efficient access to cadastre data and services, the cadastre is developing a geodetic-cadastral information system that contains extensive data on real estate, real estate addresses, and the like. Therefore, documents can be issued in electronic form through the geodetic-cadastral information system. Also, in accordance with the express provision of Article 158 of the Law, the cadastre takes care of the electronic means of providing business traffic services for the use of cadastre data and services. Like all other public administration bodies, the cadastre prescribed the introduction of electronic public administration. This is according to Article 72s, paragraph 3 of the Law on Amendments and additions The Law on State Survey and Cadastre (2015) which stipulates that electronic office operations of the cadastre with regard to requests, decisions, documents and other acts in electronic form will be established no later than March 1, 2016, except for the implementation of a unified procedure in electronic form, in accordance with the Law on Planning and Construction, the implementation of which begins on 1 of January 2016." This provision, however, has not yet taken root in practice to its full extent.

4. By-law regulations regulating certain issues of electronic administration

As it was pointed out earlier, a significant part of the issues on electronic administration, mainly of an organizational and technical nature, is left to the executive and administrative authorities to be regulated by by-laws, which are generally adopted on the basis of and in accordance with the Electronic Administration Act.

Thus, on the basis of the authorization from the Electronic Administration Act, the Government of the Republic of Serbia, in order to implement the provisions of this law, adopted the Regulation on closer conditions for the establishment of electronic administration, the Regulation on organizational and technical standards for the maintenance and improvement of the Unified Information and Communication Network of electronic administration and connecting the authority to that network, the Regulation on the way of keeping the Metaregister, the way of approving, suspending and cancelling access to the service bus of the authority and the way of working on the eAdministration Portal, the Regulation on the way of working of the Open Data Portal and the Regulation on the detailed conditions for creating and maintaining the authority's web presentation. These regulations, adopted on the basis of the Electronic Administration Act, serve to implement it, and represent parts of a coherent and unified set of regulations on electronic administration of the Republic of Serbia.

According to Article 1, the Regulation on detailed conditions for the establishment of electronic administration regulates the conditions for the establishment of electronic administration, i.e. the performance of the duties of state bodies and organizations, bodies and organizations of provincial autonomy, bodies and organizations of local self-government units, institutions, public companies, special bodies through which the regulatory function of both legal and natural persons entrusted with public authority is realized – for the purpose of establishing electronic administration.

The Regulation on organizational and technical standards for the maintenance and improvement of the Unified Information and Communication Network of Electronic Government and the connection of authorities to that network, according to Article 1 of this Regulation, regulates the organizational and technical standards for the maintenance and improvement of the Unified Information and Communication Network of Electronic Administration, which it manages the Government service responsible for the design, harmonization, development and functioning of the electronic administration system and the rules for connecting and accessing state bodies and organizations, bodies and organizations of provincial autonomy, bodies and organizations of local self-government units, institutions, public companies, special bodies through which the regulatory function is exercised and legal and natural persons entrusted with public powers on the Electronic Government Network.

According to Article 1 of the Regulation on the way of managing the Metaregister, the way of approving, suspending and cancelling access to the service bus of the authorities and the way of working on the eAdministration

Portal, this act more closely regulates the way in which state bodies and organizations, bodies and organizations of provincial autonomy, bodies and organizations of local self-government units , institutions, public companies, special bodies through which the regulatory function is exercised and legal and natural persons who are entrusted with public powers enter registers and records in electronic form in Metaregistar, determine the structure and sources of data, as well as changes, in order to ensure interoperability when obtaining, processing and assigning, that is, delivering data. This Regulation also regulates the manner of approving, suspending and terminating access to data from the registers that are connected to the Unified Information and Communication Network of Electronic Administration through the Authority's Service Bus and located in the State Centre for Data Management and Storage, as well as the manner in which authorities perform electronic administration services through the eAdministration Portal as a single access point of the electronic administration of the authority managed by the Government department responsible for designing, harmonizing, developing and functioning of the electronic administration system, terms of use, registration and work of service users on the eAdministration Portal, status monitoring related to implementation rights and obligations and other matters of importance for electronic communication with the authority through the eAdministration Portal, as well as the technical conditions of electronic delivery and the content of confirmations.

The Regulation on the operation of the Open Data Portal regulates the detailed conditions on the establishment and operation of the Open Data Portal, including organizational and technical standards, as well as other issues of importance for the functioning of the Portal – where information on open data sets is published by state authorities and organizations, authorities and organizations of provincial autonomy, bodies and organizations of local self-government units, institutions, public companies, special bodies through which the regulatory function is exercised and legal and natural persons entrusted with public powers (Article 1 of the Regulation).

The Regulation on detailed conditions for the creation and maintenance of the organ's web presentation[10] regulates detailed conditions for the establishment and operation of the Open Data Portal, including organizational and technical standards, as well as other issues of importance for the functioning of the Portal – where information on open data sets is published by the state

[10] The authors of the text of the Regulation, as well as the LGAP, mistakenly consider "web presentation of the authority" to be synonymous with the term "web page of the authority." See extensively: Milkov, 2017.

bodies and organizations, bodies and organizations of provincial autonomy, bodies and organizations of local self-government units, institutions, public companies, special bodies through which the regulatory function is exercised and legal and natural persons entrusted with public powers.

Finally, the Government of the Republic of Serbia, on the basis of its general authority to enact decrees regarding the implementation of other laws, as well as on the basis of the Law on the Government and the Law on the Planning System of the Republic of Serbia, passed the Regulation on the Office for Information Technologies and Electronic Government, as well as Program for the development of electronic administration in the Republic of Serbia for the period from 2020 to 2022 with an Action Plan for its implementation.

Thus, the Regulation on the Office for Information Technologies and Electronic Administration, according to Article 1, establishes the Office for Information Technologies and Electronic Administration (hereinafter: the Office) and determines its scope, organization and other issues relevant to its work. The office performs professional tasks related to: designing, harmonizing, developing and functioning of electronic administration systems and information systems and infrastructure of state administration bodies and government services; development and application of standards in the introduction of information and communication technologies in state administration bodies and Government services, as well as support in the application of information and communication technologies in state administration bodies and Government services; design, development, construction, maintenance and improvement of the computer network of republic authorities; tasks for the needs of the Centre for the Security of ICT Systems in the Republic's Bodies (CERT of the Republic's Bodies) and other tasks determined by the law and this Regulation.

The program for the development of electronic administration in the Republic of Serbia for the period from 2020 to 2022 with the Action Plan for its implementation is a public policy document by which the Government plans the development of electronic administration in the Republic of Serbia for that period.[11]

The aforementioned by-laws, together with the highlighted laws, represent a unique unit of legal regulation of the electronic administration system in the Republic of Serbia, and represent a necessary component for the regular functioning of this system.

[11] See in detail the text Program for the development of electronic administration in the Republic of Serbia for the period from 2020 to 2022 with the Action Plan for its implementation.

5. Concluding considerations

Based on all that has been presented, we can conclude that in the Republic of Serbia there is a broad and relatively harmonized system of legal and by-laws regulating the field of electronic administration, where the Electronic Administration Act, together with the Law on General Administrative Procedure, sets strong frameworks for further legislative interventions, especially by executive and administrative authorities in the field of electronic administration, all with the aim of establishing and managing an efficient system of electronic administration, which will smoothly and timely provide all necessary information, documents and services to citizens and the economy.

In addition, it is indicated that administrative procedures, both general and special, are slowly being digitized in our country. First of all, the Electronic Administration Act and certain provisions of the Law on General Administrative Procedure created assumptions that introduce information and communication technologies in the performance of administrative activities, and which assumptions are partially accepted in the laws governing special administrative areas.

However, there is a lot of room for improvement in this field. For the complete transformation of public administration into electronic public administration, it is necessary to enable digital management of administrative procedures. Certainly, it is not possible, by the nature of things, to digitize all administrative procedures, or even all phases of other administrative procedures, but those procedures that can be concluded with a note on the case file, without taking a statement from the parties in the procedure or in simpler one – party administrative procedures they can be completely transformed into digital form. This would lead to an even more efficient performance of administrative activities, and significant financial and time savings would be achieved, both for the parties and the acting authorities.

For a complete transition, it is necessary to ensure the security of information and data used in administrative procedures, since the integrity of citizens' personalities depends on the security of the information system and data protection. In this sphere, legislative, executive and administrative bodies must never stop taking legislative and other necessary actions.

Golić Darko
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

NORMATIVNO UREĐENJE ELEKTRONSKE UPRAVE U REPUBLICI SRBIJI

REZIME: Prateći opšti trend tehničko-tehnološkog progresa u društvu, gde tehnologija ima sve veći značaj u svakodnevnom životu, države i javne vlasti na svim kontinentima nastoje olakšati ostvarivanje i zaštitu prava svojih građana, te ukloniti birokratske barijere koje su ranije postojale i bile uobičajena prateća pojava upravnog postupka. Kao izraz takve težnje, ali i kao nužna posledica tehničkog progresa, mnoge zemlje uvode sistem elektronske javne uprave. Prateći ovaj trend, i naš zakonodavac uspostavlja sistem elektronske javne uprave, kojim nastoji olakšati ostvarivanje prava građana, ali i nastoji poboljšati sliku koju građani imaju o javnoj upravi, ranije naročito poznatoj po tromosti i neefikasnosti. Uvođenje elektronske uprave u domaći pravni sistem, pak, učinjeno bez dovoljne pripreme, nije prošlo bez izvesnih poteškoća, kako na normativnom planu, tako i na planu realizacije različitih normativnih rešenja. Ovaj rad daje prikaz pravnih propisa, odnosno normativnog okvira kojim je uređeno uvođenje i funkcionisanje elektronske uprave u Republici Srbiji.

***Ključne reči*:** *Elektronska uprava, upravni postupak, Zakon o elektronskoj upravi.*

References

1. Carinski zakon [Customs Law]. *Službeni glasnik R*S, br. 95/18, 91/19 – dr. zakon, 144/20 i 118/2
2. Đurašković, J., (2016). *Unapređenje modela efektivnog komuniciranja elektronske uprave sa privrednim društvima: doktorska disertacija* [*Improving the model of effective communication of electronic administration with companies: doctoral thesis*]. Novi Sad: Univerzitet u Novom Sadu – Fakultet tehničkih nauka

3. Henman, P., (2010). *Governing Electronically, E-Government and the Reconfiguration of Public Administration*, Policy and Power, Palgrave Macmillan, UK
4. Ivanović Knežević, J. (2013). Appeal in Tax Procedure. *Pravo – teorija i praksa*, *30*(4-6), pp. 83–95
5. Milkov D., (2017). *Upravno pravo II: upravna delatnost* [*Administrative law II: Administrative activity*]. Novi Sad: Pravni fakultet u Novom Sadu
6. Program razvoja elektronske uprave u Republici Srbiji za period od 2020. do 2022. godine sa Akcionim planom za njegovo sprovođenje [*Electronic administration development program in the Republic of Serbia for the period from 2020 to 2022 with an Action Plan for its implementation*]. *Službeni glasnik RS*, br. 85/20
7. Torbica, M. (2021). "Silence of the administration" in the administration procedure that is being instituted before the Real Estate Registry and Cable Duct Cadaster. *Pravo – teorija i praksa*, *38*(2), pp. 143-155
8. Uredba o bližim uslovima za izradu i održavanje veb prezentacije organa [Regulation on detailed conditions for the development and maintenance of the organ's web presentation]. *Službeni glasnik RS*, br. 104/18
9. Uredba o bližim uslovima za uspostavljanje elektronske uprave [Regulation on further conditions for the establishment of electronic administration]. *Službeni glasnik RS*, br. 104/18
10. Uredba o načinu rada Portala otvorenih podataka [Regulation on the manner of operation of the Open Data Portal]. *Službeni glasnik RS*, br. 104/18
11. Uredba o načinu vođenja Metaregistra, načinu odobravanja, suspendovanja i ukidanja pristupa servisnoj magistrali organa i načinu rada na Portalu eUprava [Regulation on the way of managing the Metaregister, the way of approving, suspending and cancelling access to the service bus of the body and the way of working on the eAdministration Portal]. *Službeni glasnik RS,* br. 104/18
12. Uredba o organizacionim i tehničkim standardima za održavanje i unapređenje Jedinstvene informaciono-komunikacione mreže elektronske uprave i povezivanje organa na tu mrežu [Regulation on organizational and technical standards for the maintenance and improvement of the Unified Information and Communication Network of electronic administration and the connection of bodies to that network]. *Službeni glasnik RS*, br. 104/18

13. Uredba o Kancelariji za informacione tehnologije i elektronsku upravu [Regulation on the Office for Information Technologies and Electronic Administration]. *Službeni glasnik RS*, br. 73/17 i 8/19
14. Vučinić, D., (2020). Elektronska uprava – koncept i usluge sa osvrtom na elektronsku upravu u Republici Srbiji [Elektronska uprava – koncept i usluge sa osvrtom na elektronsku upravu u Republici Srbiji[Electronic administration – concept and services with in retrospect on the electronic administration in the Republic Serbia]. *Glasnik prava*, (1), pp. 45-56
15. Zakon o državnom premeru i katastru [Law on State Survey and Cadastre]. *Službeni glasnik RS*, br. 72/09, 18/10, 65/13, 15/15 – odluka US, 96/15, 47/17 – autentično tumačenje, 113/17 – dr. zakon, 27/18 – dr. zakon, 41/18 – dr. zakon i 9/20 – dr. zakon
16. Zakon o elektronskoj upravi [Electronic Administration Act]. *Službeni glasnik RS*, br. 27/18
17. Zakon o opštem upravnom postupku [Law on General Administrative Procedure]. *Službeni glasnik RS*, br. 18/16 i 95/18 – aut. tumačenje
18. Zakonom o poreskom postupku i poreskoj administraciji[*Law on tax procedure and tax administration*]. *Službeni glasnik RS*, br. 80/02, 84/02 – ispr., ..., 86/19 i 144/20
19. Palević, M., (2020). Pravni okvir elektronske uprave u Srbiji [The legal framework of electronic administration in Serbia]. In: Mićović M. (ured.), *Usluge i prava korisnika: zbornik radova* [*Services and user's rights: collection of papers*] (pp. 523-551). Kragujevac: Pravni fakultet Univerziteta, Institut za pravne i društvene nauke

Dragojlović Joko[*]
http://orcid.org/0000-0002-4713-1855

UDK: 343.533::004
Review article
DOI: 10.5937/ptp2300063D
Received: 31.12.2022.
Approved on: 21.02.2023.
Pages: 63–83

JURISDICTION FOR CRIMINAL OFFENSES OF CYBERCRIME – INTERNATIONAL AND NATIONAL STANDARDS

ABSTRACT: Criminal acts of a computer crime are no longer a new social and legal phenomenon. In addition to the execution of criminal acts that fall within the domain of a computer crime, computers have found their application in the execution of the so-called classic criminal acts, giving them a different modus operandi. A spatial distance between the action taken and the resulting consequences during the execution of criminal acts of a computer crime, led to the strengthening of the transnational crime. Initially, the international community tried to intervene in this area, with the idea of regulating the criminal prosecution of the perpetrators of the cross-border criminal acts of a computer crime. However, to date, there has been adopted no normative framework regulating the issue of prosecuting the perpetrators of these criminal acts at the universal level. In this sense, the paper analyzes the existing international standards with regard to the normative arrangement of jurisdiction for the prosecution of perpetrators of transnational computer crimes. In addition, the paper contains a presentation of the normative arrangement of this issue in domestic legislation.

Keywords: *computer crime, transnational crimes, jurisdiction, international standards, The Convention from Budapest.*

[*] LLD, Associate professor, Faculty of Law for Economy and Justice in Novi Sad, University of the Academy of Economics in Novi Sad, Serbia, e-mail: jdragojlovic@pravni-fakultet.info

1. Introductory considerations

The immeasurably great opportunities in all spheres of social life that have appeared to man with the development of information technologies have undoubtedly entailed certain risks and social dangers that are reflected in various types of misuse of computers, computer systems and computer networks, above all the Internet.

As a consequence of the marked expansion of the use of computers and computer technologies, a new social phenomenon appeared – computer crime. It is a special type of criminality that has a very wide phenomenological dimension, bearing in mind that criminal acts are committed through computers, that is, computers are used as a means of execution, or, alternatively, as an object against which a criminal act is committed (Matijašević & Dragojlović, 2021, p. 54). Also, this type of crime has specific perpetrators, crimes are committed very quickly (in a fraction of a second), there is a large dark figure present (often the victims do not realize that they have been deceived and that one of the crimes from the area has been committed against them computer crime). In addition, with computer crime, the area of criminal activity is expanded, that is, the perpetrator can undertake an action in one country, and the consequences can occur in another, which gives this type of crime a transnational character.

Respecting all the specifics of computer crime, and especially its transnational character, the international community has a strong motive to establish a general normative framework for regulating the issue of defining computer crime and determining the rules of jurisdiction for prosecuting these crimes. However, reasons of sovereignty, political independence, interest in conducting criminal proceedings and the like prevent the international community from establishing uniform rules at the universal level, while the rules set at the regional level are not sufficiently up-to-date, not binding or not sufficiently widely set.

2. General remarks on computer crime and the question of jurisdiction in combating computer crime

Regarding the definition of computer crime, in general, it can be stated that computer crime includes both active and passive use of a computer, and even the storage of evidence of a committed criminal act in a computer or in electronic form, while the victims and possible victims are all natural and legal persons. that use or depend on computers and databases (Rome Memorandum, 2008). In this sense, the computer, as a characteristic feature of computer crime, appears in different functions: **1) the object of the execution of the**

criminal act ; **2) the subject of the criminal act** ; **3) means of committing the crime** ; **4) "weapon" or means** (Vidić, 2016, p. 94).

When it comes to the definition of computer crime itself, there is no single and generally accepted definition of computer crime in the literature. The first and most general definition was given in 1979 by the US National Law Institute in The Criminal Justice Resource Manual of computer Crime (Parker, 1989), according to which computer crime is understood as "any illegal act for which successful criminal prosecution requires good knowledge of computer technology." Such a broad definition will serve as a starting point for the international legal definition of the concept of computer crime.

From the point of view of criminal law theory, computer crime, as a general form of manifestation of various forms of criminal activity, is crime directed against the security of information (computer) systems as a whole or in its individual parts, which, in different ways and by different means, is intended to to gain some benefit for oneself or another or to cause some harm to another (Jovašević & Hašimbegović, 2004; Gordon & Ford, 2006, pp. 13-20). In this sense, Petrović and Jovašević correctly note that the key determinant of computer crime is the close connection of the criminal act with technology, from which its dynamism and variety of appearances derive (Petrović & Jovašević, 2006, pp. 211-216). We will see in the later chapter of this paper, the domestic legislator, deciding on the definition of high-tech criminality, was guided by some, but not all, of the presented theoretical legal elements of this form of criminality.

It is a generally accepted definition that the jurisdiction of an authority, in terms of criminal proceedings, implies the right and obligation of that authority to conduct and conclude one proceeding in one criminal case depending on the severity of the criminal offense, expressed in the prescribed sentence and the characteristics of the perpetrator of the criminal offense.

However, jurisdiction includes several distinct concepts, including jurisdiction to prescribe legal rules, jurisdiction to adjudicate disputes, and jurisdiction to enforce laws and decisions (Restatement, 1987, para. 401). In this sense, jurisdiction to prescribe legal rules is the authority of a sovereign entity to make its law applicable to a person's activities, relationships or status, or a person's interests in legal matters. Jurisdiction is the authority of a sovereign entity "to subject persons or subjects to the proceedings of its courts or administrative bodies" to determine whether a prescribed legal rule has been violated (Brenner & Koops, 2004, p. 5). According to the Restatement (1987, para. 401b), the power to enforce laws and decisions is the power of a sovereign entity "to encourage or compel compliance with or to punish the

violation of its laws or other regulations, whether by judicial means or by the use of executive, administrative, police or other extrajudicial measures."

Traditionally, all three manifestations of the concepts of sovereignty and jurisdiction, i.e. the three types of jurisdiction mentioned, are primarily based on the element of territoriality. Thus, from the very beginning, the state had the authority to prescribe the rules of conduct of its subjects within its physical territory, and it had the authority to enforce the prescribed rules of conduct against any individual whose illegal behavior took place on the territory of that state (Vukadinović & Avramović, 2014, pp. 38-42). This concept of jurisdiction derives from the basic principle that a sovereign entity has the legal authority to exercise control and authority over "its territory, generally to the exclusion of other states" and that it has "the power to govern its territory and the power to enforce the laws." (Restatement, 1987, para. 206b). In this sense, the US Supreme Court correctly stated that the nature of the act as a legal or illegal action must be determined entirely by the law of the country where the act itself was committed (American Banana Company v. United Fruit Company). From the foregoing, therefore, it follows that no state and no sovereign entity can apply its criminal laws to behaviors that occur on the physical territory of another nation.[1]

However, the constant development and expansion in the use of information and telecommunication technology significantly undermines certain assumptions that gave birth to the traditional model of jurisdiction, as an expression of sovereignty (Goodman & Brenner, 2002, pp. 4-24). The development of technology has made it much easier to commit a criminal offense in one country, while the victim, i.e. the injured person, is physically located in another country, which all creates new and unique challenges in the area of jurisdiction for prescribing and prosecuting criminal offenses of computer crime, but also raised the question of the need to revise the regulations on extradition. In this sense, the existing concept of requiring double criminality of the act for legal extradition, as well as the position that states have sovereign power over those within their borders, still retain their

[1] True, this principle is deviated from in the criminal legislation in certain cases. Likewise, the provisions on the territorial validity of the Criminal Code of the Republic of Serbia (Articles 7–9 of the Criminal Code) provide for the validity of this criminal regulation for acts committed abroad. However, Article 10 of the CC provides for relatively strict conditions for the application of the previous provisions on territorial validity. Therefore, these narrowly constructed exceptions, as well as the rules on universal jurisdiction for the prosecution of certain criminal acts incriminated at the international level (e.g. genocide, war crimes, etc.), should not be understood as violating the general principle of the limited validity of the criminal legislation of a country only on the territory of that country, without affecting, at the same time, the legal rules on extraterritorial areas.

importance, but in the past few decades there has been a need to review and relativize these attitudes regarding the exercise of criminal jurisdiction.[2]

Jurisdiction, therefore, no longer depends only on the physical presence of a person on the territory of a country. However, even under this expanded view of jurisdiction, a state cannot "exercise jurisdiction to prescribe rules of conduct in relation to a person or activity connected with another state when the exercise of such jurisdiction would be unreasonable (Restatemen 1987, para 403(1)).[3]

So, as can be concluded, the appearance of computers, computer systems and computer networks, as well as their development and the expansion of the use of these novelties, caused changes in the previous approaches to jurisdiction for trial in criminal matters, because the previous concepts, mostly based on the principle of territoriality, they could no longer maintain as absolute.

3. International standards regarding jurisdiction for prosecuting criminal offenses of computer crimes

Bearing in mind the fact of the spread of information technologies and, consequently, computer crime, as well as the importance of suppressing this phenomenon and the consequences it causes, it is not surprising that the

[2] Namely, in order for extradition to be legal and possible, as a rule, it is required that extradition can only be carried out if there is a so-called "dual criminality" which means that one and the same act is criminalized in both countries as a criminal offense. If, on the other hand, this is not the case, but only one country incriminates the act, then the other country, which does not incriminate the act, will not, as a rule, be able to carry out a legal extradition. On the problem of extradition on the example of the computer virus Love bug from 2000, see in detail: (Brenner & Koops, 2004, pp. 7-8).

[3] Whether the exercise of the power to prescribe is unreasonable is determined by taking into account various factors, including the following: (a) the connection of the activity with the territory of the regulating state, that is, the extent to which the activity takes place within the territory, or has a significant, direct and foreseeable effect on or in the territory; (b) links, such as nationality, residence or economic activities, between the regulating State and the person principally responsible for the activity to be regulated or between that State and the one the regulation is designed to protect; (c) the character of the activity being regulated, the significance of the regulation to the regulating state, the extent to which other states regulate such activities, and the degree to which the desirability of such regulation is generally accepted. (d) the existence of legitimate expectations that could be protected or harmed by the regulation; (e) the importance of the regulation for the international political, legal, or economic system; (f) the extent to which the regulation is in accordance with the traditions of the international system; (g) the extent to which another state may have an interest in regulating the activity; and (h) the likelihood of conflict with the regulations of another state (Restatement 1987, para 403(2)) The standard of reasonableness is, in paragraphs 3 and 4 of the same article of the Restatement, used to determine jurisdiction to try and enforce judicial and extrajudicial decisions. This standard, however, is not without problems.

international community, both at the universal level, within the United Nations, and at regional levels (Council of Europe, European Union), intervened in the field of computer crime. Consequently certain international documents in the field of high-tech crime, which foresee criminal acts and mechanisms by which these acts can be prevented, also determine the rules on jurisdiction for the prosecution of these criminal acts. The most detailed and relevant, certainly, is the Convention on High-tech Crime.

It can be stated that significant progress has been achieved on the international level with regard to the normative regulation of computer crime, but that there are still significant problems related to international cooperation and global efforts to combat computer crime.[4]

4. International standards contained in United Nations documents

As part of the work of the General Assembly, the United Nations adopted several resolutions dedicated to computer crime.[5]

Work in the field of legal regulation of computer crime The United Nations began in 1990, when the Resolution on legislation in the field of computer crime was adopted at the VIII UN Congress on the Prevention of Crime and the Treatment of Offenders (8th UN Congress on the Prevention of Crime and the Treatment of Offenders) held in Havana. After the adoption of this Resolution, in 1994, the OUN Manual on the prevention and control of computer crime was adopted, and then in May 1998, the Geneva Resolution on the abuse of the Internet for the purpose of sexual exploitation. The Geneva resolution stated that the Internet is currently the most unregulated communication network in the world with new technologies that represent a major challenge for national and international regulation and application, and warned that various forms of sexual exploitation are being promoted on the Internet for the purpose of sexual entertainment. In order to reduce these phenomena, the Resolution contains

[4] The most important problems are: different legal definitions of the actions of computer crime; insufficient training of police officers, prosecutors and judges who act in cases of computer crime; inconsistency of procedural rules in criminal laws when it comes to the investigation and prosecution of computer crimes; non-functioning or absence of international legal assistance. See more: (Bejatović, 2012, p. 22).

[5] These resolutions, it is true, do not have binding force for the member states and are mostly declarative in nature, but they should be mentioned because they contain a call to all states to harmonize legislation in this area as soon as possible in order to eliminate the so-called "safe states" for computer crime in which harmful behaviors related to misuse of computers, information and communication technologies are not criminalized and sanctioned (Vidić, 2016, p. 256).

recommendations to influence the reduction of human trafficking, prostitution and sexual exploitation on the Internet. [6]In 2000, the General Assembly of the United Nations adopted the Resolution on the fight against misuse of information technologies. This Resolution highlights the importance of certain measures in the fight against misuse of information technologies.[7]

At the 10th Congress of the United Nations in 2005, which was dedicated to crime prevention, a working group of experts defined computer crime as a general term that includes criminal acts committed through computer systems or networks. This means that this term includes any criminal offense committed in the electronic environment (Matijašević & Ignjatijević, 2010, p. 853). In the plenary part of the session dedicated to computer crime, it was stated that it is possible to recognize two types of computer crime (Nikić, 2010): (1) computer crime in the narrower sense, which includes any illegal behavior aimed at the electronic security operations of computer systems and the data processed in them (which includes acts related to unauthorized access to a computer system or network by violating security measures; damage to computer data or programs; computer sabotage; unauthorized interception of communications from and in computer systems and networks; computer espionage), (2) computer crime in the wider sense, which includes any illegal behavior related to or in relation to a computer system and network, including such criminality as the illegal possession, offering and distribution of information through computer systems and networks (such as computer forgery; computer theft; technical manipulation of devices or electronic skim components of the device; abuse of

[6] In the recommendations, the governments of the signatory countries and non-governmental organizations are suggested to, as a priority, consider amendments and implementation of existing laws or pass new laws in order to prevent the abuse of the Internet for trafficking, prostitution and sexual exploitation of women and children; classes investigation related to the misuse of the Internet for the purposes of promoting and/or conducting trade, prostitution and sexual exploitation of women and children; undertake more vigorous measures in order to eliminate human trafficking, exploitation of prostitution and sexual exploitation on the Internet; develop educational programs, policies and laws regarding the use of the Internet by users of prostitution; conduct an investigation and use as a record of criminal acts and acts of discrimination advertising, correspondence and other forms of communication over the Internet that are used to promote sex trade, prostitution, sex tourism, bride trafficking and rape; develop good cooperation at the level of national and regional bodies of criminal services in the fight against the escalation of trafficking and prostitution of women and children, the globalization of this industry and the abuse of the Internet to promote and implement acts of sex trafficking, sexual tourism, sexual violence and sexual exploitation.

[7] Two measures are listed as the most important measures: the first is that states must provide such laws and practices that will eliminate any possible "sanctuary" for those who misuse information technologies in the criminal sense; and secondly, that the legal system must protect and respect the confidentiality, integrity and availability of electronic data and computer systems, so that their abuse and unauthorized use do not occur and that every perpetrator of such a crime is sanctioned.

payment systems such as manipulation and theft of electronic credit cards or use of false codes in illegal financial activities).

As can be concluded from this brief overview, it is clear that there is still no universal convention or any other act that comprehensively regulates the issue of cyber and computer crime, but the regulation is limited to recommendations, manuals and the like. On the other hand, efforts within the UN are mainly focused on substantive criminal law, that is, prescribing a unique definition of certain forms of computer crime, while defining jurisdiction for prosecuting these crimes is, for now, on the back burner.

However, with the increasingly widespread occurrence of computer crime, and attacks directed at the computer systems and databases of various governments and international organizations, while the perpetrators of these acts are as a rule outside the jurisdiction of the injured states or international organizations, namely the United Nations, therefore, announced the imminent adoption of the text of the universal convention on cybercrime.

In our opinion, when regulating this issue, the United Nations should, as a starting point, take the Convention of the Council of Europe on high-tech crime no. 185 from 2001, and the concept of obligation and rules to preserve national sovereignty should be regulated according to the model of the UN Convention on Combating Transnational Organized Crime.

5. Standards contained in the documents of the Council of Europe – Budapest Convention

Convention no. 185 adopted within the framework of the Council of Europe in 2001, after several years of work on harmonizing the integral text of this convention.

Council of Europe Convention on High-Technological Crime 185 from 2001, Additional Protocol to the Convention on High-Technological Crime, which refers to the criminalization of acts of a racist and xenophobic nature committed via computer systems (Strasbourg, 28.01.2005), as well as the Second Additional Protocol to the Convention on High-Technological Crime to crime related to enhanced cooperation and the discovery of electronic evidence [8]are the

[8] The second additional protocol to the Convention on High-tech Crime was adopted, after several years of negotiations on the text of this Protocol, in November 2021, and was opened for signature in May 2022; For now, this Protocol has been signed by 24 countries (18 members of the Council of Europe and 6 non-member states, including the USA), but no country has yet ratified this Protocol. The entry into force of the Protocol is subject to ratification by five countries. The Republic of Serbia has signed, but not yet ratified, this Protocol.

first international documents which, on a broad level, regulate the substantive, organizational, procedural and international framework of criminal offenses committed via the Internet and other computer networks. The adoption of these documents is the result of a Council of Europe initiative formally launched in 1996 with the establishment of the Committee of Experts on Cybercrime. The convention is an international legal instrument that for the first time regulates problems related to high-tech crime and modern media (Dragojlović & Krstinić, 2015, p. 95).

The convention has as its goal, first of all, the harmonization of domestic substantive criminal law provisions in the field of computer crime, enabling the domestic criminal procedural legal framework to provide competent state authorities with the powers necessary for the effective detection and prosecution of perpetrators of these crimes, as well as the establishment of a quick and effective framework of international cooperation in this area. The provisions of the Convention are systematized in four chapters: the first chapter defines the concepts, the second, foresees the measures that need to be taken at the level of individual states within the framework of criminal substantive and procedural legislation, the third chapter refers to international cooperation within the framework of mutual assistance in the fight against computer crime and the fourth relates to the final provisions of signing and entry into force (accession, territorial application, declarations, reservations, settlement of disputes, cancellation, etc.). The importance of the Convention lies primarily in the fact that its adoption enabled national legislations to develop their own network of combating computer crime based on the provisions of the Convention (Vidić, 2016, p. 265).

When, on the other hand, we talk about the rules on jurisdiction for prosecuting computer crimes, the Convention devotes only one article to this issue: Article 22 of the Convention.

According to the provision of this article, paragraph 1, each "Contracting Party should adopt legislative and other measures necessary to establish jurisdiction for each act prescribed in accordance with articles 2–11 of this Convention, when the act is committed:

a) on its territory; or
b) on a ship under the flag of that contracting party; or
c) in an aircraft registered in accordance with the laws of that contracting party;
d) by its citizen, if the act is punishable under the criminal law of the country where it was committed or if the act was committed in a place outside the jurisdiction of any country."

From the above, it can be clearly determined that, in this paragraph, the Convention sets as a general rule, and insists on it, jurisdiction according to the traditional principle of territoriality[9] – the contracting state will have jurisdiction when the act was committed on its territory, accepting, at the same time, the rules on extraterritorial places and jurisdictions of the state. This approach, although theoretically and legally correct, which stems from the concept of sovereignty, can no longer be accepted in modern conditions.

It is true that point g) of this paragraph allows the contracting state to prosecute its citizen for an incriminated offense that he committed abroad, but only if that offense is double incriminated – that it is prescribed as a criminal offense both in the country that wants to undertake the criminal prosecution of his citizen, as well as in the state where the act itself was committed. Also, the state will have jurisdiction to prosecute even if the crime was committed in an area that does not fall under the jurisdiction of any other state.[10] However, these rules on criminal jurisdiction are, in our view, part of the generally accepted legal principle regarding criminal jurisdiction and the interest of each state, and represent the usual "expansion" of the criminal jurisdiction of a country, and not specific rules on the jurisdiction of this Convention.

Thus, adapting and more extensively understanding the concept of territoriality, the Report (para. 233) points out that, according to Article 22, paragraph 1a, the contracting state could establish territorial jurisdiction if both the perpetrator (attacker of the computer system) and the attacked system are located within the territory of that country (which is the

[9] The report should not be understood as an authentic interpretation of the Convention. However, it is de facto an authoritative source of law. This is because in practice preparatory reports, notes and drafts from sessions where the text of any international agreement (fr. Travaux preparatoires) was prepared are regularly used as a means of interpreting the agreement or determining the intention of the contracting parties. In this sense, Article 32 of the Vienna Convention on the Law of Treaties foresees preparatory works as a way of interpreting an international treaty.

[10] It is interesting to point out that, according to the Report (para. 235), "the area that does not fall under the jurisdiction of any other country" should primarily be understood as the area that is outside the borders of the planet Earth – that is, space and, analogously, space bodies. As, according to customary international law, as well as the corresponding documents of the United Nations, no country can establish jurisdiction in space, and it is the good of all humanity, in the event that a cyber attack is carried out outside the space of the planet Earth, the jurisdiction to prosecute that act would every country had. This solution, as well as the far-reaching view that its authors had, can only be criticized in terms of resolving conflicts of jurisdiction in the event that when the act is possible to be done in outer space, and it is done, what will happen if several states establish your jurisdiction? This is because this Convention does not establish a clear mechanism for resolving conflicts of jurisdiction, except for the provision of paragraph 5 of the same article, according to which the contracting parties will "consult" regarding the determination of the most suitable jurisdiction for prosecution.

application of the classical principle of territoriality), but the state will have the authority to prosecute even when only the attacked computer system is located within the territory, regardless of whether the perpetrator of the act (according to the Report – the "attacker") is not located on the territory of that country. This approach can be justified from two aspects. First, the very nature of computer crime, which often has an international element, dictates the expansion of the traditional concept of territorial jurisdiction. Especially in modern times, it is relatively common for attacks on computer systems in one country to come from the territory of another country. If the requirement that both the attacked system and the attacker should be located on the territory of the same country, in order for it to have jurisdiction, would remain, the efforts of the international community to combat transnational computer crime would be significantly obstructed. In addition, such type of criminal activity would not need to be regulated at the international level – it would be the domain of exclusive national jurisdiction. In addition, the general interest of the international community, embodied through various international and regional organizations, is not to intervene and regulate the internal issues of each country, but to normatively regulate those issues that are of international importance, that have an international element, that is, that concern several countries. On the other hand, it is a theoretically legally acceptable position regarding extended territorial jurisdiction if the moment of the committed act is taken into account. Namely, criminal acts of computer crime, as a rule, are not consequential crimes. Therefore, it is not required that the damage actually occurred, or that the data was actually changed. For the existence of a crime, it is sufficient that a breach in the computer system (hacking) has occurred. Even the penetration of the computer system represents damage in itself, and the deed is completed.[11] Therefore, although the opposite could be argued, we believe that, bearing in mind the peculiarity of computer crime, it can be considered that the consequence of the action – hacking – occurred on the territory of the country where the specific computer system is located. In addition, the

[11] This does not mean that there are no other criminal acts that incriminate different behavior and that contain additional or broader elements of the criminal act. Thus, there are also those criminal acts that require a special element of intent – for example, Article 300 of the Serbian Criminal Code provides for the act of creating and introducing computer viruses, and where the existence of the criminal act is conditioned by the existence of intent – the act of creating a computer virus with intent is criminalized its entry into someone else's computer or computer network. However, it is not necessary that the introduction of the virus actually occurred, nor that it was attempted. For the existence of a criminal offense, it is sufficient to prove that the virus was created and that the intention to introduce it existed.

country in whose territory the computer system that is attacked has the strongest interest in prosecuting the attackers of that computer system. For all the reasons stated, this determination of the authors of the Convention is completely acceptable, reasonable and justified.

When it comes to the rules on extraterritorial places and jurisdiction, paragraph 2 of Article 22 of the Convention stipulates that each Contracting Party may retain the right not to apply, or to apply only in certain cases or under certain circumstances, the rules on jurisdiction specified in paragraphs 1b) to 1g) of this article or in another part of that article. The linguistic interpretation alone easily leads to the conclusion that this provision allows the contracting states to express reservations in relation to the rules of jurisdiction in these cases, in such a way as to completely exclude the application of these rules, or to partially exclude them, or to bind their application to occurrence of any additional condition (Report, para. 238). However, the contracting states cannot exclude, limit or condition the application of the rule of territorial jurisdiction from point a) of this paragraph, considering that the exclusion of that basis of jurisdiction would completely defeat the purpose of international regulation of this issue.

Each Contracting Party should adopt the measures necessary to establish its jurisdiction over the acts listed in Article 24, paragraph 1 of this Convention, after submitting a request for extradition, in cases where the suspect is on its territory and the Contracting Party only of his or her citizenship, shall not be extradited to the other contracting party (Article 22, paragraph 3 of the Convention). This provision embodies the general legal principle of public international law *aut dedere aut judicare* (extradite or prosecute). In the case when the contracting party refused to extradite the alleged perpetrator of the crime prescribed by the Convention on the basis of his nationality, and the perpetrator is present on its territory, it was necessary to prescribe the jurisdictional rule from paragraph 3, to ensure that those states that refuse to extradite citizens have the legal possibility to, instead of extradition, undertake investigation and prosecution, if requested by the contracting state that requested extradition in accordance with the rules of "Extradition", from Article 24, paragraph 6 of this Convention (Report, para. 238). This rule, therefore, preserves the basic principle of international law – deliver or judge. In addition, if one member state could refuse both extradition and trial for the offense provided for in the Convention, then neither the Convention itself nor the international regulation of the fight against international computer crime would have any meaning or purpose. That is why the obligation provided for in this provision is, by its very nature, an objective obligation – states

are obliged to adopt the measures necessary to preserve the *extradite or try principle.*

According to paragraph 4 of Article 22, this Convention does not exclude jurisdiction for any criminal prosecution undertaken in accordance with domestic law. As already pointed out, this Convention was adopted after several years of consultation and harmonization of the draft of its text. In addition, it represents a compromise of different countries, different systems and political interests. In addition, this Convention aimed to establish a minimum of uniform rules in this area. That is why, in this position, it has been established that the rules on the bases of jurisdiction set forth in this article are not *numerus clausus,* that is, they are not of an exclusive nature, and the contracting parties are essentially free to, in accordance with their internal criminal legislation, establish other bases and types of criminal jurisdiction (Report , para. 238).

When several Contracting Parties assert jurisdiction over an alleged act prescribed in accordance with the Convention, those Contracting Parties shall consult each other, when appropriate, regarding the determination of the most appropriate jurisdiction for prosecution (Article 22, paragraph 5 of the Convention). Therefore, as it was pointed out earlier, this Convention, taking into account all the circumstances in which it was adopted, does not contain a concrete mechanism for resolving conflicts of jurisdiction. That is, there are no clear rules according to which the dispute will be resolved if two or more states simultaneously establish jurisdiction in relation to the same offense and the same perpetrator. According to the explanation from the Report (para. 239), it can be concluded that the idea was that, in the case when several of them establish jurisdiction, they will agree on where to prosecute and for which offense, all guided by the rational interests of easier enforcement investigations, prosecutions, evidence, etc. However, this explanation seems more like an effort to justify the prescribed rule as completely reasonable and logical, and not as a result of the impossibility of political compromise. It is completely clear that no country wants to give up its jurisdiction, as an expression of its sovereignty. Each state will therefore have an interest and a desire to prosecute the perpetrator of an act directed against it, its order and its subjects. However, it is also a reality that at a given moment it was necessary to first make a step forward in the fight against computer crime at the international level, and during the adoption of this Convention a compromise was made regarding the rules on jurisdiction. This is all the more so since even the consultations prescribed by paragraph 5 of Article 22 are not mandatory in every case of jurisdictional disputes, but will only take place “when it is

appropriate." This, further, means that if State A considers that consultations are expedient, and State B considers that they are not, consultations will not take place (Report, para. 239).

In truth, with the special and extensive rules on international cooperation contained in the Convention (Articles 23-35 of the Convention), the authors of the Convention tried to replace the relatively loose rules on jurisdiction with extensive rules and obligations on international cooperation. This effort is further embodied in the 2021 Second Additional Protocol on Enhanced Cooperation and Discovery of Electronic Evidence.

The Budapest Convention certainly represented the first and important step in the right direction towards universal regulation of the issue of combating and suppressing international computer crime, which is more relevant today than ever. In addition, this Convention laid the foundations for individual national legislations to more precisely determine the features and characteristics of individual computer crimes, their basic, easier or more serious forms, and to prescribe criminal sanctions for their perpetrators (natural or legal entities) (Jovašević, 2014, p. 41).

6. National standards regarding competence for prosecuting criminal offenses of computer crimes

When it comes to domestic legislation, it is necessary to look at the issue of computer crime from the aspect of assumed international obligations and from the aspect of the internal regulation of normative and institutional regulation of the issue of jurisdiction for the prosecution of criminal acts of computer crime.

Regarding the aspect of assumed international obligations, the Republic of Serbia signed the Council of Europe Convention on High-tech Crime and the Additional Protocol back in 2005, and finally ratified them in 2009, without reservations or declarations. In addition, the Republic of Serbia signed the Second Additional Protocol to this Convention in May 2022, but it has not yet been ratified. The Republic of Serbia hereby undertakes to prescribe and establish normative and institutional prerequisites for successfully combating computer crime.

To that end, several regulations (laws and by-laws) were adopted in which certain provisions of the Convention were implemented and on the basis of which an institutional framework was created for their implementation. The most important among them are the following laws: the Law on the Organization and Competence of State Bodies for Combating High-Tech

Crime[12], the Criminal Code of the Republic of Serbia and the Criminal Procedure Code of the Republic of Serbia.

The Law on the Organization and Competence of State Bodies for Combating High-Tech Crime is undeniably the most important legal document in the fight against this type of crime in Serbia (Dragojlović & Krstinić, 2015, p. 98). This Law determines the institutional framework for the implementation of the provisions of the law related to high-tech crime, and it foresees special organizational units of existing state bodies, whose actions contribute to better protection against computer crime and the implementation of preventive and repressive measures. The specialization of state authorities to fight against computer crime is necessary due to the complexity and special characteristics of computer crime, the necessity of special knowledge in this area (Dragojlović & Krstinić, 2015, p. 98) as well as due to the constant monitoring of the development of modern computer technologies.

Special rules on jurisdiction refer to special state bodies that are responsible for detecting, prosecuting and adjudicating high-tech crimes. This primarily refers to special units within the Ministry of Internal Affairs, the Special Prosecutor's Office for High-Tech Crime, as well as the rules on jurisdiction. Thus, the Law on the Organization and Competence of State Bodies for Combating High-Tech Crime, Article 4, Paragraph 1 prescribes that the Higher Public Prosecutor's Office in Belgrade is responsible for handling cases of criminal offenses from this law for the territory of the Republic of Serbia, while Paragraph 2 of the same Article prescribes that a special department for the fight against high-tech crime be formed in the High Public Prosecutor's Office in Belgrade (hereinafter: Special Prosecutor's Office). According to Article 5, the work of this Special Prosecutor's Office is managed by the High-Tech Crime Prosecutor, who is appointed for a period of four years by the Public Prosecutor of the Republic, with the consent of the appointed person. This Prosecutor has all the rights and obligations of a public prosecutor (according to the latest amendments to the Constitution of the RS,

[12] According to Article 3, this Law is applied for the purpose of detection, prosecution and trial of criminal offenses against the security of computer data specified in the Criminal Code and – criminal offenses against intellectual property, property, economy and legal traffic in which the object or means of execution of criminal offenses occur computers, computer systems, computer networks and computer data, as well as their products in material or electronic form, if the number of copies of copyrighted works exceeds 2,000 or the resulting material damage exceeds the amount of 1,000,000 dinars, as well as criminal offenses against human freedoms and rights and citizen, sexual freedom, public order and peace and constitutional order and security of the Republic of Serbia, which due to the method of execution or the means used can be considered criminal acts of high-tech crime.

he is the Chief Prosecutor). On the other hand, the provisions of Article 10 and 11 of the Law define the jurisdiction and organization of courts in terms of trials for criminal offenses within the scope of this Law. Thus, Article 10, Paragraph 1 stipulates that the High Court in Belgrade is competent for dealing with cases of criminal offenses from this law, for the territory of the Republic of Serbia, while Paragraph 2 determines that the Court of Appeal in Belgrade is competent for decision-making in the second instance. [13]Article 11, on the other hand, stipulates that the High Court in Belgrade shall establish a (special) Department for the fight against high-tech crime in the High Court in Belgrade to deal with cases of criminal offenses from this Law, which will consist of judges appointed by the President of the High Court in Belgrade from among the judges of that court , for a period of 2 years, and with their consent.

With regard to the organization and competence of the internal affairs body, as an investigative body, in Article 9 of the Law on the Organization and Competence of State Bodies for Combating High-Tech Crime, the Office for the Fight against High-Tech Crime is established for the work of the internal affairs body in cases related to these crimes which is located within the Ministry of Internal Affairs, and which acts according to the requests of the Special Prosecutor.

So, as we can see, with this Law, the concentration of jurisdiction was carried out both in terms of the actions of the prosecution, as well as in terms of the actions and trials of the court, by this regulation deviating from the general rules of local jurisdiction contained in the Code of Criminal Procedure by jurisdiction is concentrated in the High Public Prosecutor's Office in Belgrade and the High Court in Belgrade, with their special departments. In practice, there are no major problems in determining the competence for the actions of special departments. In addition, although it is not explicitly determined by this Law, the High Court in Belgrade is the only one competent to provide international legal assistance in criminal acts of high-tech crime, in the sense of the Budapest Convention. This approach, according to the author, could be initially accepted, taking into account the fact that high-tech crime was not so widespread at the time of the adoption of the first law in this area (2005). However, in modern times, the prevalence of computer crime, which our

[13] It was completely unnecessary, in our opinion, to determine that the appellate jurisdiction belongs to the Court of Appeal in Belgrade. Since the High Court in Belgrade (in a special department) judges in the first instance, it is quite logical that the Court of Appeal in Belgrade will also have jurisdiction over the appeal, which is also a general rule contained in the Law on the Organization of Courts. Therefore, the inclusion of this provision in a separate law cannot be justified.

legislator defined even more widely than the international standard, is so great that it would be completely justified, if not necessary, to establish appropriate special departments of the prosecution and courts in Novi Sad, Kragujevac and Nan, and in that sense, a partial deconcentration of jurisdiction should be implemented, and as it was done also with regard to organized crime.

7. Conclusion

Computer crime certainly represents one of the biggest security challenges of the twenty-first century, both for developed and less developed countries. Effective prevention, detection and initiation of proceedings against perpetrators of criminal offenses is further hampered by its transnational character.

The international community, due to different interests, which mostly rest on the sovereignty of each state, has not yet established minimal uniform rules on a universal level that would regulate some issues in the field of cybercrime. The Council of Europe, as a regional organization, has, we have seen, intervened and adopted the Convention on High-Tech Crime, with two additional protocols. However, even within these documents, the question of jurisdiction is loosely regulated, precisely because of the absence of the will of the contracting states to renounce their jurisdiction for criminal acts of computer crime. There, as the biggest problem, the issue of resolving conflicts of jurisdiction may arise when one of the states claiming jurisdiction does not consider it expedient to participate in the consultations. Protection of the national interest, the principle of sovereignty and jurisdiction for criminal prosecution as an expression of the same, are certainly high values that the state should protect. However, the danger of transnational cybercrime is immediate and high, and this circumstance must have an impact on the attitude of countries regarding the prosecution of these acts prescribed by the Convention. The idea of establishing a European tribunal for high-tech crime, with complementary jurisdiction, does not seem completely unacceptable either – if the states fail to agree, through consultation, on which of them will exercise jurisdiction. Certainly, it is necessary for the international community to settle this issue in the shortest possible time in the most comprehensive way.

When it comes to our country, Serbia, by ratifying the Convention and the Additional Protocol and incorporating its provisions into the national legislation, has shown a clear will and readiness to fight against high-tech crime, and the normative solutions in Serbia in this area represent a good basis for leading a successful fight against this type of crime. criminality. Also, the existing

normative solutions are harmonized to a significant extent with European standards, i.e. with the Convention and the Additional Protocol. However, in the future, we should work on strengthening the technical-technological and personnel conditions for detecting and prosecuting these crimes. In addition, *de lege ferenda,* our legislator should carry out a partial deconcentration of jurisdiction from Belgrade to Novi Sad, Kragujevac and Niš.

Dragojlović Joko
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

NADLEŽNOST ZA KRIVIČNA DELA RAČUNARSKOG KRIMINALITETA – MEĐUNARODNI I NACIONALNI STANDARDI

REZIME: Krivična dela računarskog kriminaliteta ne predstavljaju više novu društvenu i pravnu pojavu. Pored izvršenja krivičnih dela koja spadaju u domen računarskog kriminaliteta, računari su svoju primenu našli i kod izvršenja tkz. klasičnih krivičnih dela, dajući im drugačiji modus operandi. Prostorna distanca između preduzete radnje i nastale posledice prilikom izvršenja krivičnih dela računarskog kriminaliteta, doveli su do jačanja transnacionalnog kriminala. Inicijalno, međunarodna zajednica je nastojala intervenisati u ovoj oblasti, sa idejom da uredi krivično gonjenje učinilaca prekograničnih krivičnih dela računarskog kriminaliteta. Međutim, do danas nije usvojen normativni okvir koji će na univerzalnom nivou urediti pitanje gonjenja učinilaca ovih krivičnih dela. U tom smislu, u radu je izvršena analiza postojećih međunarodnih standarda u pogledu normativnog uređivanja nadležnosti za gonjenje učinioca transnacionalnih računarskih krivičnih dela, a pored toga, dat je i prikaz normativnog uređenja ovog pitanja u domaćem zakonodavstvu. Cilj ovog rada je da ukaže na poteškoće koje nastaju prilikom regulisanja nadležnosti kod krivičnih dela računarskog kriminaliteta, kao i analiza postojećih nedostataka i ukazivanje na eventualne pravce budućeg regulisanja.

Ključne reči: *računarski kriminalitet, transnacionalna krivična dela, nadležnost, međunarodni standardi, Konvencija iz Budimpešte.*

References

1. Bejatović, S. (2012). Visokotehnološki kriminal i krivičnopravni instrumenti suprotstavljanja [High-tech crime and criminal legal instruments of opposition]. In: Šikman M. (ured.), *Suzbijanje kriminala i evropske integracije s osvrtom na viskotehnološki kriminal* [*Suppression of crime and European integration with reference to high-tech crime*]. (pp. 17-30), Banja Luka: Visoka škola unutrašnjih poslova
2. Brenner, S. W., Koops, B., J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*, *4*(1), pp. 3-46
3. Dragojlović, J., & Krstinić, D. (2015). Evropski standardi u borbi protiv visokotehnološkog kriminaliteta i njihova implementacija u zakonodavstvu Republike Srbije [European standards in the fight against high-tech crime and their implementation in the legislation of the Republic of Serbia]. *Evropsko zakonodavstvo*, *14*(51), pp. 92-103
4. Goodman D., M., & Brenner W., S., (2002). The Emerging Consensus on Criminal Conduct in Cyberspace, *International Journal of Law & Technology*, *10*(2), pp. 139-223
5. Gordon, S., Ford, R. (2006). On the definition and classification of cybercrime, *Journal of computer virology*, *2*(1), pp. 13-20
6. Jovašević, D. (2014). Računarski kriminalitet u Srbiji i evropski standardi [Cybercrime in Serbia and European standards]. *Evropsko zakonodavstvo*, *13*(47-48), pp. 40-56
7. Jovašević, D., & Hašimbegović, T. (2004) Krivičnopravna zaštita bezbednosti računarskih podataka [Criminal Protection of Computer Data Security]. In: Petrović, R., (ured.), *Zloupotreba informacionih tehnologija i zaštita* [*Misuse of information technologies and protection*] (pp. 1-9). Beograd: Udruženje sudskih veštaka za informacione tehnologije
8. Konvencija Saveta Evrope o visokotehnološkom kriminalu br. 185 [Convention on Cybercrime CETS No. 185], 23. 11. 2001
9. Krivični zakonik [Criminal Code]. *Službeni glasnik RS*, br. 85/05, 88/05 – ispr., 107/05 – ispr., 72/09, 111/09, 121/12, 104/13, 108/14, 94/16 i 35/19
10. Matijašević, J., & Ignjatijević, S., (2010). Kompjuterski kriminal u pravnoj teoriji, pojam, karakteristike, posledice [Cybercrime in legal theory, concept, characteristics, consequences], In: *Infoteh Jahorina*, (pp. 852-856), Istočno Sarajevo: Elektrotehnički fakultet u Istočnom Sarajevu

11. Matijašević, J., & Dragojlović, J., (2021). Metodika otkrivanja krivičnih dela računarskog kriminaliteta [Methodology of detection of computer crime offenses], *Kultura polisa*, 18 (posebno izdanje 2), pp. 51-63. DOI: 10.51738/Kpolisa2021.18.2p.1.04
12. Nikić, S., (2010). Najčešće metode napada cyber kriminalaca i kako se odbraniti [The most common methods of attack by cybercriminals and how to defend yourself]. In: Petrović, R., (ured.), *Zloupotreba informacionih tehnologija i zaštita* [*Misuse of information technologies and protection*]. (pp. 265-279). Beograd: Udruženje sudskih veštaka za informacione tehnologije
13. Parker, D., B., (1989). *The Cybercrime: Criminal Justice Resource Manual*, Washington: National Institute of Justice
14. Petrović, B., Jovašević, D. (2006). Izvršno krivično/kazneno pravo [Enforcement criminal/penal law]. Sarajevo: Pravni fakultet
15. Priručnik UN o sprečavanju i kontroli kompjuterskog kriminala [United Nations Manual on the Prevention and Control of Computer-related Crime], 1994. Downloaded 2022, September 15 from https://www.unodc.org/pdf/Manual_ComputerRelatedCrime.PDF
16. Report and Guidance on Privacy in Social Network Services – "Rome Memorandum" – 43rd meeting, 3-4 March 2008, Rome (Italy). Downloaded 2022, September 15 from https://www.gpdp.it/documents/10160/10704/1531476
17. Restatement (Third) Of Foreign Relations Law Of The United States (1987). Downloaded 2022, September 16 from https://www.ali.org/publications/show/foreign-relations-law-united-states-rest/
18. Rezolucija Ujedinjenih Nacija A/res/55/63 o borbi protiv zloupotrebe informacionih tehnologija [UN resolution A/res/55/63 on combating the criminal misuse of information technologies], 04. 12. 2000
19. Rezolucija Ujedinjenih Nacija o zakonodavstvu u oblasti kompjuterskog kriminaliteta [UN Resolution on computer crime legislation], 07. 09. 1990.
20. Vidić, V. (2016). *Povreda prava na privatnost zloupotrebom društvenih mreža kao oblik kompjuterskog kriminaliteta – doktorska disertacija* [*Violation of the right to privacy by abuse of social networks as a form of cybercrime – doctoral dissertation*]. Niš: Pravni fakultet
21. Vukadinović, G., & Avramović, D. (2014). *Uvod u pravo* [*Introduction to Law*]. Novi Sad, Pravni fakultet

22. Zakon o organizaciji i nadležnosti državnih organa za borbu protiv visokotehnološkog kriminala [Law on Ratification of the Convention on High-Tech Crime]. *Službeni glasnik* RS, br. 61/05 i 104/09
23. Zakonik o krivičnom postupku [Code on Criminal Procedure]. *Službeni glasnik RS*, br. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14, 35/19, 27/21 – odluka US i 62/21 – odluka US

Stojšić Dabetić Jelena[*]
http://orcid.org/0000-0002-3229-837X

UDK: 347.4:004.738.5
Review article
DOI: 10.5937/ptp2300084S
Received: 31.01.2023.
Approved on: 12.02.2023.
Pages: 84–98

WRAP CONTRACTS AND THEIR INFLUENCE ON THE CONTRACT LAW

ABSTRACT: The basis of the digital economy is electronic commerce (e-commerce), based on contracting which increasingly relies on the use of a digital technology. A contract represents the basis of legal obligation, as well as the foundation of the validity and legitimacy of legal rules, dating back to the theory of the social contract. The functioning of the digital society and digital economy has introduced the process of digitization into the scope of the Contract Law and contracting practice. On the example of wrap contracts, as a kind of online contracts by access (adhesion contracts), the author shows how new practices in contracting affect the traditional obligation law institutes.

Keywords: *contracting, wrap contracts, the Contract Law, digital society, declaration of will.*

1. Introduction

Modern society, defined as digital society, introduces a new reality into market relations through new and different forms of offering goods and services, primarily electronically and with the usage of new terminology in economy and law. Consequently, the contracting processes go through changes, in the broader context of digital economy as the dominant framework of market exchange in the digital society, in form of electronic commerce. One

[*] LL.D, Associate Professor, The Faculty of Law for Commerce and Judiciary in Novi Sad, The University Business Academy, Republic of Serbia, e-mail: j.stojsic.dabetic@gmail.com

of the novelties is, for example, that the courts appear as creators of standards of fairness that apply to consumers in the case of contracts concluded over the Internet, since courts can respond to the regulatory needs of modern commerce faster than the legislator. This trend indicates that the creation of new regulation in all areas of law affected by the use of digital technology is based on case law, i.e. the principles of precedent law. Furthermore, different forms of online, i.e. electronic trading, introduce new ways and standards of assessing the consent of the buyer, i.e. consumer to the transaction. Payment for goods and services in various crypto currencies is accepted. Thus, today we are witnessing to digital technology changing the basic principles of traditional fields of law, including contract law, and two regulatory processes are taking place in parallel – the revision of traditional principles of contract as well as other fields of law, on the one hand, and the creation of new, innovative normative solutions on the other.

The author's intention in this paper is to engage in an analysis of the normative consequences of the usage of digital technology in contracting, and thus also of the interaction of law and digital technology on the example of a narrow legal issue such as online adhesion contracts or wrap contracts, and in the broader context of digital society, digital economy and the development of electronic commerce. The paper is segmented into three separate central parts, in addition to introduction and conclusion, that complement each other and consequently derive from each other. The first part shows the specific phenomenology of contracting in the digital society, with an emphasis on online adhesion contracts, and serves as a closer background for the analysis that follows in the second and third parts of the paper. The second part of the paper is dedicated exclusively to wrap contracts as a special type of contracts which are concluded precisely with the usage of digital technology and which are one of the forms of electronic contracting that is most commonly used among users of digital technology. The third part of the paper is a normative analysis and examination of the scope of the application of traditional contract law institutes and principles in the context of the implementation of wrap contracts. The concluding part of the paper indicates the potential impacts of the regulation of the use of digital technology in contracting on the redefinition of contract law, in the broader context of the digital economy and digital society.

2. Phenomenology of contracting in the digital society

Contemporary development of economic activity in the form of digital economy shows that contracts in business transactions are concluded with the wide usage of the services of the information society. Electronic commerce implies the conduct of transactions electronically, primarily using the Internet as the dominant business environment for the promotion of goods or services, as well as for the conclusion and execution of contracts (Dukić Mijatović & Mirković, 2022, p. 54). A complete purchasing of goods today can be made via the website, from ordering, through payment and even delivery of the requested goods as digital content (Mirković & Stojšić Dabetić, 2020, p. 60). Merchants who use the Internet or other forms of information society services for their business can establish special electronic, automated representatives who receive orders on their behalf, as special electronic representatives. This form of purchasing appears as the most convenient from the aspect of timeliness and financial benefit, both from the point of view of the buyer and the seller.

The usage of digital technology in the daily business practice of contracting individuals and legal entities has led to a change in the consciousness of individuals regarding contracting. Before the use of digital, or electronic, devices, it was virtually impossible for an individual to be bound by a contract without being aware of it, in the sense that they had not read it or otherwise agreed to it. The dominant form of contract was a written contract, where each contracting party, before signing the contract, took the time to read the contract and be informed of all the legal consequences of its conclusion. This is precisely the contractual phase when lawyers or other legal advisors participate in the conclusion of the contract and provide legal assistance to the parties. With the usage of digital technology in contracting, very often we are not even aware that we have entered into contractual relationship, that we are a contracting party, and thus an obligated party, in relation to another, most often, legal entity. This is a consequence of the management of transactions and business and every other communication predominantly via electronic means (Gutbrod, 2020). For example, every time we buy juice, coffee or other goods from a vending machine into which we insert money or a card in order to pay, we have concluded a sales contract. Also, every time we click on the button “Accept all cookies” or “I agree” to view the content of a website, we, again, become a contracting party, although we did not give monetary compensation, but access to our data instead.

Precisely this type of communication that takes place online between the user and the provider of a digital service is based on different forms of

contractual relations, mainly in the form of online adhesion contracts, which are concluded on a daily basis and often individuals are not even aware that they clicking on icon or other act made them enter into a contractual relationship (Grundmann & Hacker, 2017). The daily practice of concluding contracts on the Internet for most users means easily agreeing to their content, often without even reading and not knowing that they are actually entering into an agreement that expresses the legally relevant agreement of the will of the contracting parties. In this sense, the most common way of concluding a contract on the Internet is not by a signature (not even an electronic one), often it is not an express consent as such drawn up in a verbal sense, but a conclusive action, which represents an act by which one contracting party (the user) enters into a certain contractual relationship under often pre-offered and pre-defined conditions of the information society service provider. Therefore, every action on the Internet where person selects an item or service, or where goods or services are ordered, puts the user in the position of a contracting party, with all the rights and obligations that this status entails in the legal sense. A step further in the arrangement of contractual relations on the Internet are contracts in electronic form, which are usually drawn up beforehand and presented to the user who, by clicking on a specific link or checkbox button for marking, confirms agreement with their content and thus "signs" it.

It has become common practice to use automated software on websites that are used for sales, in which the parameters for receiving orders are pre-set (programmed) and this enables orders to be placed without the seller's knowledge. In such cases, the sale is made through classic adhesion contracts concluded through the website, where the software acts as an electronic representative of the seller. Contracts where declarations of will are made by electronic means can be characterized as reactive in the sense that they require an additional communicative action from the contracting parties in order to complete the contracting. It can be a click on a certain field on the web page (clickwrap contracts), which means the completion of the contracting process, or by accessing the web page itself (browsewrap contracts). In other words, in the digital context, the offer can be created as open one, that is addressed to any Internet user through open communication channels, e.g. via the website, or it can be limited in the sense that it is sent to a certain number of users in a personalized way via email or even encrypted. Acceptance of the offer is at the same time the moment of concluding the contract, either by clicking on a specific field on the website (with an additional step of confirmation with the next click), by filling out the form on the website or by email.

3. Online adhesion contracts – wrap contracts

Contracts by access or adhesion contracts are contracts that have a predetermined content, to which the other contracting party may or may not agree. These contracts are most often concluded by individulas with banks, mobile operators, utility service providers, etc., as standardized contracts, the content of which is predetermined by one contracting party, which decides on the conditions for concluding the contract and which offers the pre-created contract to the other party or parties for signing. Although they are often criticized, adhesion contracts in practice have significant advantages: lower costs (in the sense that all transactions of the same type are performed in the same way) and less time consuming, the conditions contained in the contracts have passed the "test" of the court and are one of the the most suitable instruments for mass transactions. Pre-prepared form contracts speed up the process of negotiation and conclusion of the contract, and are characteristic in situations where a large number of contracts are concluded between the offeror and the various offered contractual parties, bearing in mind that the content of the contract has already been written, and certain changes can possibly be made if there is an agreement of the contracting parties. The most obvious disadvantage of these contracts relates to the position of the other party, that is, the acceding party who did not participate in determining the terms contained in the contract. Most often, a situation occurs where the person entering the contract gives priority to the benefit he receives from the contract, even though he may not fully agree with the terms contained in the contract he is entering.

General terms and conditions of business (Terms of Service) are an integral part of the adhesion contract (which are adopted by the contractual party that drew up the contract), and they can be implemented in the contract itself, or the contract only refers to them. The general terms and conditions, unless something else has been agreed, produce the same legal effect towards the contracting parties as the contract itself, provided that the offered contracting party is familiar with them in the usual manner. General conditions, in a broader sense, represent the conditions under which some companies operate. They are an integral part of the contract, and are usually found on the back of the contract form or under the signed part of the text.

When comes to defining an online adhesion contract, as a special form of adhesion contract, it can be defined as a contract that regulates the mutual relationship between the user and the Internet service provider (Internet service provider – ISP). Every type of usage of Internet, that is, visit to a certain website

implies consent to the terms of use of that page, which are precisely contained in the online adhesion contracts that are commonly called wrap contracts. In practice, a large number of users are not aware of the existence of such conditions, nor that they are contained in the legal form of the contract and that their actions in relation to them corresponds to the conclusion of a contract and the acquisition of the status of a contracting party, that is, that they entered into a contractual relationship by undertaking a certain act. The problem with adhesion contracts in general is that the contracting party, the accessing party, is often not aware that has entered into a contractual relationship at all, which is more pronounced in the case of wrap contracts that are concluded online. Today, in modern business surroundings, this type of contract is so common at the daily level of an individual's interaction that individuals do not even notice that they have entered into a contract, especially if they conclude this contract online.[1]

In practice, wrap contracts are the ones that enable access to the website with prior acceptance of the Terms of Service (ToS). In this type of contract, the expression of will in the online context determines the relationship with the ISP, and the ISP gives notice of the contract and the consequences of the user's behavior. Nevertheless, despite this, the main problem with this type of contract is that the users most often do not know that they have entered into a contractual relationship and are not aware of the consequences of their declaration of will, or that they have given a valid declaration of will. In the context of the contractual relationship between the user and the online service provider (provider or platform), wrap contracts are the only effective practice that benefits both parties. The most common issues contained in the terms of these contracts relate to software licensing, terms of use of the website, choice of competent court, i.e. possible arbitration clause and applicable law, copyright, issues of data security, privacy and return of goods. "Take it or leave it" clauses play a significant role in the creation of wrap contracts, the conditions of which are determined and published by the ISP, and in the online context this is the only way to formulate a contract. These clauses are often very brief, more detailed content is usually available via links, and users are often unaware of the extent of the content of the contract they have entered into. Common content that users may become familiar with through the terms of use are terms of sale, software licensing, choice of court, arbitration

[1] In the case of adhesion contracts that are concluded offline, there is usually a third party, an expert, who can point out all the consequences of the contract to the weaker party, that is, the party that approaches. In the online context of concluding such contracts, the aforementioned practice is simply absent and the accessing party is usually left to its own assessment of the situation, and consequently is often unaware that it has entered into a contractual relationship.

clauses, copyright, security, choice of rights, etc. In any case, there must be reasonable notice of the existence of the terms of use, which in the event of a dispute is assessed in relation to its placing in the website, font size and type, terms and words used, presentation, form and functionality, web design, color, hyperlinking, user experience – therefore according to the assessment of subjective and objective factors.

Online adhesion contracts are in practice, but also in theory, referred to as *wrap contracts*. The term wrap corresponds to the way in which the accessing party, that is, the user, expresses the will to commit, that is to access them (Klasiček, 2021, p. 174). Wrap contracts are defined as non-negotiable digital contracts, and belong to the category of contracts by access or adhesion contracts (Kim, 2020). There are three basic types of wrap contracts – shrinkwraps, clickwraps and browsewraps, including various hybrid forms of these contracts that appear in practice (click-browse wrap hybrids, scroll wraps, sign-in wraps, multiwraps: shrink-clickwrap hybrid or shrink-click-browse wrap hybrids).

Shrinkwrap contracts are contracts that are an integral part of the packaging or the purchased product itself – usually software. The user, i.e. the party accessing the contract, becomes familiar with the contract by opening the plastic or other type of packaging, i.e. the wrapper. This is the only type of wrap contract that has a written, i.e. printed form, and it is considered that the party entered into the contract by opening the packaging, that is, by removing the packaging, which means that the moment of opening the packaging represents the moment of concluding the contract (Radovanović, 2008, p. 679). Consent is expressed by opening the packaging, and in practice this means that the user first gives his consent and then familiarizes himself with the content and conditions of the contract. And this is the biggest drawback of this type of contract, and the contract usually stipulates a certain time limit for the user to return the software and withdraw from the contract, although not as a general rule.

Clickwrap (click-accept, click-to-sign) contracts imply that the accessing party declares its consent directly, and it is assumed that the accessing party is aware of entering into a contractual relationship. The user declares himself by clicking on the field related to the statement "I agree", "I disagree", "OK" or similar. It is especially important to point out in connection with this type of contract that the user cannot continue using the website or other content if he does not agree to the terms of use. And it can be said that in digital circumstances this is one form of the most direct expression of consent, even though it does not have its own physical form (Matić, 2008, p. 790). In the case of this type of contract, the contract itself contains terms that define the

way the user interacts with the digital service. In this case, users are presented with all terms of the contract in advance.

In practice, the clickwrap contract is displayed to the user as a separate screen that prevents the user from continuing to view or use the content unless it is confirmed by clicking or otherwise that the user has familiarized himself with the terms of use presented within the screen. This type of contract doesn't ever have a physical form, unlike a shrinkwrap contract, but the user is given the opportunity to familiarize himself with all the terms of use before giving his consent. In practice, cliskwrap contracts have been subject to criticism because users were often unaware that they were agreeing to the terms by clicking, since very few users actually read the entire text contained within the screen (Benoliel & Becher, 2019). On the other hand, the websites themselves and other platforms strive to create content that keeps the attention of users and often avoids explicit emphasis on legal consequences. For this reason, users are often unaware that they are entering into a legally binding relationship and that a legal obligation has arisen for them after clicking. If it can be proven that the user made a click, the contract is considered valid, regardless of whether the user has actually read the conditions to which he agreed, whether he understood them and whether he is aware of entering into a legally binding relationship. The only argument with which the user can defend himself in the case of a proven click is by claiming that the terms of use are not in accordance with public order and the principles of good business, or in accordance with general contractual rules.

Browsewrap contracts are a type of adhesion contract where the user is least aware that he has entered into a contract at all. These agreements are "hidden" behind a hyperlink located on a website or other platform. Most often, there is a notice on the page itself that by visiting the page or downloading content from it, the user agrees to the terms of use on a contractual basis. In practice, this is a situation that the user is aware of to a very small extent, especially if he enters into a contractual relationship just by navigating the website. These agreements apply to access or use of content on the website or in connection with a product downloaded from the website. The user can familiarize himself with all the conditions and content of the contract only after clicking on the hyperlink. If the internet provider provides adequate notification to the user that by moving around the page or downloading content from the page, he creates a contractual relationship, that is, consent to the terms of use, then the browsewrap contract has legal force and is enforceable.

When using wrap contracts in practice, especially in relation to contracts that regulate the relationship between users and websites or other digital

platforms in connection with the use of content – clickwrap and browsewrap contracts, problems arise in connection with the manifestation of consent. Business practice has indicated the need to redefine traditional contractual standards related to the expression and content of consent, as well as the standards of responsibility of the contracting parties. The terms of use of the website may be available via browsewrap, in the sense that the user can access them by clicking on the hyperlink, but is under no obligation to do so, although further use of the page, i.e. access to the page, requires acceptance of the terms of use. If special conditions of the use of website are relevant, they must be sufficiently visible to the ordinary careful user. Otherwise, they are not applicable. Regardless of the existence of sufficiently visible notice of the applicability of the terms of use, it is necessary to prove the existence of an affirmative action that unequivocally proves individual consent to the contract (Kim, 2021). Jurisprudence clearly pointed out that the mere fact of using the website cannot be considered as consent to the terms of use. In the event that consent cannot be proven, the courts are not inclined to rule in favor of the existence of a contract, i.e. acceptance of the terms of use. In case that user's attention has not been clearly drawn to the material conditions, i.e. in a way that would be understandable to an objectively prudent user, the conditions of use could not be applied in the specific case. The terms of use of the website are not binding for the user if a reasonably visible notice wasn't available or visible to the user, to which the user has given unequivocal consent. If there is no requirement for affirmative consent, such as checking the box, and the user was not warned of the conditions either by a different font, letter size or other mechanism, users cannot be considered bound by the terms of use (Daiza, 2018, p. 215). The website by its design must provide a reasonably visible notice that a specific action undertaken by user while on the page will result in entering into a contractual relationship. Even when purchase is conducted through the website, it must be clearly emphasized that the purchase entails consent to the terms of use, and possibly the choice of applicable law or competent court, limitation of the seller's liability, etc. Also, it must be clearly indicated that installing, accessing or using certain software, e.g. if it is not necessary to accept the general conditions for downloading games, the general conditions cannot be considered as binding. The site administrator must prove that the notification about the conditions of use, i.e. the consequences of using the website, is really visible, also in the case where the continued use of the website implies an expression of will, that is, that the site administrator interprets and accepts the continued use as consent. The notice on the terms of use is analyzed from the perspective of the site

user, and is the responsibility of the site administrator, i.e. the creator of the contract. Terms of use and other notices that entail the emergence of legal obligations must be such that they attract the attention of a reasonable user, that is, a normally prudent user of the website. When contracts are created by using websites, in the event of a dispute, it is necessary to determine whether the design and content of the website interface allow access to the terms of use, i.e. notice of the consequences of use, and whether the terms of use are formulated and presented in a clear and visible manner. In the event of a dispute, the court analyzes the visual presentation of the terms of use, and on this basis determines the responsibility of the website. When creating web pages that offer services or sell software, users should at the same time be provided with easy access to the content of the page and be informed in an appropriate manner about the consequences of using the page in terms of legal obligations. Also, the terms of use are subject to change, and if one wants to successfully refer to them, the website must prove that the user was familiar with them, that is, that he was aware of the changes made in a timely manner.

The responsibility of the contractual parties is first of all appreciated from the perspective of the website user who, by visiting the website and using the content of the website, knowingly or unknowingly enters into a contractual relationship. The visibility of the text itself, which either contains the terms of use or refers to them, is evaluated, as well as the process during which the terms of use are presented to the user. In the practice of USA courts, the courts have most often analyzed successive screenshots called "webflows" or "flows" in order to understand the path by which the user gets acquainted with the terms of use and to assess whether the process of entering the website itself warns the user that a contract has been concluded by making certain actions on the page itself (Kim, 2020, p. 1692). The practice of courts in the USA puts the burden of proof on the contractual party that made the contract to prove its quality, i.e. the suitability of webflow at the moment when it claims that the user agreed to the terms of use, as well as to prove that the user actually visited the page during that period.

4. Specific questions relating to online wrap contracts

The phenomenology and specifics of wrap contracts that arise in the digital environment have been previously exposed. At this point, it is advisable to give a general overview of the traditional contract law rules that refer to wrap contracts, and at the same time point out the specifics that exist in this sense in the context of wrap contracts, as online adhesion contracts. Wrap contracts are

contracts where one party pre-determines the elements and conditions of the contract through a general and permanent offer, and the other party only accesses such an offer without the possibility of any negotiation. The conclusion of these contracts is not preceded by negotiation as a separate phase of the contracting cycle. They are an expression of restrictions on the freedom of contract that relate to the content of the contract, but they are, in addition, one of the most commonly applicable types of contract in legal transactions (Hart, 2014, p. 107). The generality of the offer in this type of contract implies that the offer is addressed to an unspecified and unlimited number of persons and that each person can accept the offer in its entirety. After acceptance, the content of the offer becomes the content of the contract. The constancy of the offer implies that the party, that is, the offeror constantly repeats it, which means that the offer results from the regular and permanent activity of the offering party.

The conditions under which this type of contract is concluded are called "general conditions" or "terms of use" and for the contract to be valid it is essential that the general conditions at the time of conclusion of the contract were or had to be known to the party accessing them. In the case of these contracts, the inequality of the parties, primarily economic, is obvious, but this characteristic does not enter into the legal features of the wrap contract, that is, it is not a legally relevant fact, but only explains them from an economic aspect. Wrap contracts are also referred to as formulary agreements, but they are not formal agreements, with the obligation to publish the general terms and conditions in a legally prescribed manner so that the other party can adequately familiarize with them. The party that draws up the contract usually includes general conditions into it, either through a formulary contract or by referring to them, with the obligation that those general conditions are previously published in a usual way that allows the other party to become familiar with them in a timely and complete manner. The generally accepted rules of contract law concerning these contracts include, among other things, the duty of the court to interpret them, in the event of a dispute, in favor of the party accessing them. Therefore, the party that claims that it was not aware of the general conditions at the time of concluding the contract must also prove it. The general conditions must be in accordance with good business practices, and this first of all implies that the party who accesses them must not be placed in a difficult and unfair position, and if they prove to be null and void, the entire contract will be nullified.

Presented legal outline of wrap contracts makes them particularly suitable for contracting in a digital business environment, and also for daily regulation of the use of certain forms of digital technology and information society services. The context of the wrap contract complicates the issue of

expressing consent because the existence of adequate notification by the digital service provider as well as the expression of the user's consent must be determined in particular. For example, when talking about the declaration of will of the contracting parties in the context of wrap contracts concluded online, the most explicit declaration of will exists in the case of a clickwrap contract, and the least in the case of a browsewrap contract. Shrinkwrap contracts are characterized by at least a direct declaration of will, that is, it is contained in the act of removing the packaging. Regardless of the form of the wrap contract, the notice on the terms of use must be presented to the user as clearly as possible, as well as the consequences of his actions on the website or in another digital context. A notice that is considered legally adequate can be directly exposed or be presented in a form that allows a reasonably careful, that is, a conscientious user to become familiar with it and be aware of its existence and consequences. In judicial practice, this means the way this notice is presented, what is the position of the notice, the size and font used in the text, the choice of words, the presentation on the page, the design of the page, hyper linking and generally the general impression of the user experience are taken into account. It is the obligation of the digital service provider to fulfill these conditions in relation to the assessment of the conscientious user. Also, at the same time, the digital service provider must clearly present the user with the consequences of his expression of consent in this context, again according to the standards of a conscientious user.

5. Conclusion

The law governing electronic contracts is constantly and rapidly changing and being redefined. Standards related to notices and expressions of consent still apply, but are applied in a different way compared to electronic contracts, especially the so-called wrap contracts. The legal validity of the notice of consequences is evaluated in relation to the perspective of the users of the page and the way in which their creator decided to present them. Instead of asking the question why the user did not read the terms of use, the question is increasingly asked why the provider did not present the terms in a sufficiently visible way – website owners must make the terms they want to oblige their users sufficiently visible. In the event of a dispute, the creator of the page must show how he made the terms of use available and that the user was actually on the website when the terms were presented.

There are perceptions that traditional contractual principles are flexible enough to apply in the digital environment. Institutes of traditional contract

law, such as changed circumstances, conduct in accordance with the principle of conscientiousness and honesty and obligations of consideration towards the contractor are flexible enough to be interpreted according to each specific situation. However, it is impossible to apply the algorithmic code to open legal standards such as bona fides or force majeure, good business practice, protection of the weaker party, that is, some conditions cannot be evaluated by the algorithm for the purposes of application. The standards of "due diligence" and "declaration of consent" remain the same in their content and effect, but the manner of application of those standards depends on the circumstances of the specific case. Courts have begun to take into account and appreciate the appearance of the website and how the creator of the page decides to present the terms of use of the page – the burden of proof is transferred to the creator of the page.

Rapid development of the digital economy requires the creation of a coherent and global legal framework, especially in relation to guarantees of legal protection when using digital technology. The goal of legal regulation is to achieve a balance between minimizing the risk of digitalization and legitimizing new assets, especially in digital form, in terms of digital content and digital services, i.e. digital assets. From the standpoint of states, as well as at supranational levels, primarily under the auspices of international organizations, efforts are being made to develop strategies that adapt law to the usage of digital technology. And this is the direction established today between law and digital technology – law has to adapt to the new reality of using digital technology, as we have seen being done in the context of contract law nowadays.

Stojšić Dabetić Jelena
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

WRAP UGOVORI I NJIHOV UTICAJ NA UGOVORNO PRAVO

REZIME: Osnov digitalne ekonomije jeste elektronska trgovina (e-trgovina), čiji je osnov ugovaranje, koje se u sve većoj meri oslanja na upotrebu digitalne tehnologije. Ugovor je osnov pravnog obavezivanja, osnov važenja i legitimiteta pravnih pravila, počeviši od teorija društvenog

ugovora. Funkcionisanje digitalnog društva i digitalne ekonomije uvelo je proces digitalizacije u ugovorno pravo i praksu ugovaranja. Na primeru wrap ugovora, kao svojevrsnih onlajn ugovora po pristupu (adhezionih ugovora), autorka prikazuje kako nove prakse u ugovaranju utiču na tradicionalne obligacionopravne institute.

Ključne reči: *ugovaranje, wrap ugovori, ugovorno pravo, digitalno društvo, izjava volje.*

References

1. Benoliel, U., Becher, S. (2019). The duty to read the unreadable, *Boston College Law Riview*, (60), pp. 2255–2296
2. Daiza, H. (2018). Wrap Contracts: How They Can Work Better for Business and Consumers, *California Western Law Review, 54*(1), pp. 201-239
3. Dukić Mijatović, M., & Mirković, P. (2022). Digitalna ekonomija i informaciono društvo – domet i pristup pravne regulacije [Digital economy and informational society – scope and approach of legal regulation]. *Ekonomija – teorija i praksa*, *15*(2), pp. 53–70
4. Grundmann, S., & Hacker, P. (2017). Digital technology as a challenge to European Contract Law. *European Review of Contract Law*, *13*(3), pp. 255–293
5. Gutbrod, M., (2020). Digital Transformation in Economy and Law, *Digital Law Journal*, *1*(1), pp. 12–23
6. Hart, D. (2014). Form & Substance in Nancy Kim's Wrap Contracts, *Southwestern Law Review*, *44*(2) pp. 251-265
7. Kim, N. (2020). Digital Contracts, *The Business Lawyer*, *75*(1), pp. 1683-1694
8. Kim, N. (2021). New Developments in Digital and Wrap Contracts, *The Business Lawyer*, *76*(1), pp. 1-13
9. Klasiček, D. (2021). Declarations of will in the digital environment and wrap contracts, *Zbornik radova Pravnog fakulteta u Nišu*, *60*(92), pp. 173-194
10. Matić, T. (2008). Formularni ugovori u elektroničkom obliku, [Formulary contracts in the electronic form] *Zbornik PFZ*, *58*(3), pp. 779-803
11. Mirković, P., & Stojšić Dabetić, J. (2020) Alternativni načini organizovanja privrednog poslovanja za vreme pandemije Covid 19 – izazovi elektronske trgovine, [Alternative ways of organization of business activities during

the covid-19 pandemic – challenges of electronic trade] *Kultura polisa, 17*(2), pp. 55–68.
12. Radovanović, S. (2008). Ugovori o licenci softvera na omotu proizvoda (nove forme zaključenja ugovora), [Software license agreements on product packaging – new forms of contract conclusion]. *Zbornik radova Pravnog fakulteta u Novom Sadu*, (1-2), pp. 677-694.

Vasić Milica[*]
https://orcid.org/0000-0002-5964-3524
Bulatović Petar[**]

UDK: 347.714:004
Review article
DOI: 10.5937/ptp2300099V
Received: 20.11.2022.
Approved on: 02.02.2023.
Pages: 99–113

DIGITAL TRANSFORMATION OF THE BUSINESS REGISTERS AGENCY IN THE FUNCTION OF THE MODERN DIGITAL SOCIETY

ABSTRACT: Digitalization strongly affects the economy and society as a whole in different dimensions. The process of digitalization of the Business Registers Agency, including the registration procedure of business entities, is one of the priority tasks aimed at increasing efficiency and economy as well as economic prosperity in general. Certainly, there is a prerequisite referring to the existence of digital literacy, which is not an isolated category, but rather a superstructure of earlier forms of literacy. It is undeniable that every innovation arises as a privilege of the higher social classes, which, by inertia, turns into a need of the others. In this paper, it has been analyzed the legislative framework of electronic registration of business entities. Starting from the point of view that economic growth, competitiveness on the market, and socio-economic development represent the nowadays necessity, the authors, through this paper, primarily try to define the achieved progress of the work of the Business Registers Agency (BRA) in registering business entities in the digitalization process. The quintessence of this work is the identification of the availability of digital tools for the registration of economic entities, as well as their quantification and qualification.

[*] LLM, PhD candidate and teaching assistant at the Faculty of Law for Commerce and Judiciary, The University of Business Academy in Novi Sad, Serbia, e-mail: milica.vasic@pravni-fakultet.info
[**] PhD, Assistant with PhD at Belgrade Business and Arts Academy of Applied Studies, Serbia, e-mail: petar.bulatović@bpa.edu.rs

Keywords: *digital society, the Business Registers Agency, registration, digital economy.*

1. Introduction

Dynamic business conditions as a prerogative initiate constant changes and the implementation of digitalization as a business orientation of all market participants. The digital world is no longer characterized as a revolutionary phenomenon but is seen as a permanent state of evolution. The proliferation of the Internet has had a great impact on society. Therefore, it is unquestionable that the Internet represents the key to communication and the information infrastructure that primarily dictates the pace of work. While factories were the trademark of the industrial revolution, the emblem of digitalization is the symbiosis of information and computers. The potential brought by digitalization has created space for the advancement of the digital economy at the micro and macro levels. The core of digitalization is the transformation of business processes, which starts linearly from digital communication, where it is also the most noticeable.As the digital revolution unfolded, the digitalization of the economy accelerated networking and information exchange but also encouraged international engagement. The rise of the digital economy is parallel to the growth of the networked society. The trend towards the globalization of innovation is part of the general tendency of business entities to acquire technology externally and to cooperate with other companies, universities, and public research organizations, in addition to internal investments in research, development, and innovation activities.

The discourse of the defined research rests on the deductive analysis of the Business Registers Agency digitalization, which is reflected in a better understanding, and in increasing the degree of practical use of the electronic registration of business entities.

The digitalization process of the business entity registration procedure must be carried out by the current legal regulations. It is of crucial importance to consider the extent to which the existing legal regulations enable the effective implementation of this procedure. The subject of the research paper is the analysis of the relevant legislative framework for the corpus of issues regulation related to the electronic registration of business entities in the Business Registers Agency. The purpose of the research is in direct correlation with the subject of the research, that is, the identification of current legal regulations, as well as the recognition and analysis of relevant legal issues related to the digitalization of the registration of business entities. The theoretical

and professional analysis of the electronic registration of business entities will indirectly reflect the enormous role of digitalization in the development of the economy and economy, as well as raising the public services quality level.

2. Research methods

Following the chosen issue, the applied research methodology is based on legal-dogmatic and empirical methods.

The legal-dogmatic method implies a normative analysis of the positive legal regulation, which has as its subject the registration of economic entities, as well as whether the established legal framework is suitable to respond to the challenges of digitization. The normative analysis goal is the conceptualization of the Business Registers Agency digitalization, as well as the procedure of registration of business entities using digital technology, as abstract concepts.

The empirical part of the research includes relevant and available data analysis on the registration of economic entities by the method of direct observation on the Business Registers Agencywebsite, to draw relevant scientific and professional conclusions about the identification of digital elements that are part of the Agency's work.

3. Results

The level of digitalization integrated into the business entities' work processes varies. Some countries have digitalized the entire life cycle of the company, while in others physical presence before the competent authority is necessary, at least once.

The sedes material for the considered area is in the Law on the Procedure of Registration in the Business Registers Agency. Through the normative analysis of the relevant regulations, it was established that the procedure for registering business entities and the register is under the competence of the Business Registers Agency, which represents an electronic and centralized database. The Business Registers Agency was founded in 2004. Thus, the reform implementation of the system of registration of business entities in the Republic of Serbia started, to harmonize its legislation with European standards and pave the way for foreign investments and economic prosperity of the Republic of Serbia. With this, a transition was made from the judicial way of keeping the register to a centralized, administratively more rational, and efficient one within the Agency. Furthermore, the system of financial leasing registration and liens on movable property and rights was established. One of the relevant

characteristics is that the Business Registers Agency does not enter the budget of the Republic of Serbia, which reflects the principle of self-sustainability of public functions, with the simultaneous relaxation of the state budget.

The Agency is responsible for maintaining several registers as unique, centralized, and public databases, which opens the door for state bodies and institutions to be informed in one place about the relevant data of registered business entities.

It is of fundamental importance to mention the Directive on the use of digital tools and processes in company law, based on which the establishment of companies and their registration, reduced costs, time, and administrative burdens associated with those processes have been simplified. According to the Directive, each country should decide which procedures to do online when establishing business entities. Certainly, the current costs and burdens associated with the establishment and registration procedures arise not only from the administrative fees charged for the establishment of a company or the registration of business entities but also from other requirements that make the overall process longer to complete, especially when the physical presence of the applicant is required. In addition, information about such procedures should be available online and free of charge (Directive 2019/1151).

Digitalization provides electronic access to the database, which facilitates access to important data. By establishing an integrated database, state authorities, as well as other institutions, have been provided with the use of concise and complete data and information in one place for analysis, diagnosis, and creation of fiscal and monetary policy. It certainly contributed to the economy, efficiency, and transparency of keeping the register. By creating the website of the Business Registers Agency, registered data and documents could become public and accessible to all persons.

Configuring a corporate and stable framework for the registration of business entities contributes to the unification of the business market. In 2011, the Republic of Serbia adopted the Law on the Procedure of Registration in the Business Registers Agency, with the latest amendments from 2021 (hereinafter referred to as the Law). With the adoption of the Law, the procedure for registration, recording, and publication of data and documents is regulated by legislation, which, under a special law, is the subject of registration, records, and publication in the registers and records maintained by the Business Registers Agency.

Electronic registration of business entities was made possible for the first time in Serbia through the Business Registers Agency in 2017. It primarily meant only the registration of entrepreneurs, and from the end of

2018, the registration of the establishment of a single-member limited liability company, while in 2019 this possibility was also allowed for a multi-member limited liability company. According to Article 9 of the Law, the application for registration of business entities can be submitted electronically, in addition to the regular paper form. The novelty of crucial importance, which the Law brings by prescribing paragraph 2, in Article 9, refers to the establishment of a business company, for which the application for the establishment will be submitted exclusively in electronic form in the future. The Legislator's motive for such a change is manifested in the need to digitalize the economy, among other things, through the e-government platform.[1]

The entire mindset transformation was carried out by configuring the software solution, which enabled the submission of electronic applications. The concept of the digital economy requires continuous growth and innovation in the work of economic entities, which directly excludes the perverted and slow work of the state administration.

Through the normative analysis of the Law on the Procedure of Registration in the Business Registers Agency, it is established that the electronic application for registration is made through a user application.By the user application, electronic documents are securely received, including proof of payment of the registration fee. Signing the electronic application is done by electronic signature.

According to the deductive analysis of Article 2, paragraph 1, of theLaw on Electronic Document, Electronic Identification and Trust Services in Electronic Business, an electronic signature represents a set of data in electronic form that are associated or logically connected with other signed data in electronic form so that it is confirmed by an electronic signature the integrity of that data and the identity of the signatory. The information required for the creation of an electronic signature is the identified data of the signatory for the creation of an electronic signature logically connected with the corresponding data for the validation of the electronic signature. When the electronic application is received, the electronic signature is validated. Validation is the procedure of checking data related to the correspondence of the electronic signature with the signed data. Validation of the qualified electronic signature on the application or documents is performed according to the time of receipt, i.e. the time of loading the documents into the user application and is confirmed with a qualified electronic time stamp. The legislator standardized the qualified

[1] It is a process that takes time to implement, which is why the implementation of this solution has been postponed until May 17, 2023.

electronic time stamp in the Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business, which is issued by the provider of the qualified trust service, as an official time attached to the data in an electronic form confirming that the data existed then.

With the adoption of the Law on Amendments to the Law on the Procedure of Registration in the Business Registers Agencyon 16 November 2021. year, the Legislator prescribed that the digitalization of the document and the confirmation of identity to the original required for the registration procedure, in addition to the persons established by the Law on Electronic Documents, Electronic Identification, and Trust Services in Electronic Business, can also be performed by a lawyer registered in the lawyers'list of the Bar Association of Serbia. With his electronic signature, that is, with a qualified electronic seal, he simultaneously signs the application with which that act is submitted.On that occasion, the lawyer signs the application with his electronic signature, i.e. with a qualified electronic seal, at the same time. The lawyer is obliged to keep the original act, i.e. the document that he digitalized and submitted to theBusiness Registers Agency, as well as the digitalized act itself. An enormous number of registration applications are submitted to the Business Registers Agency by lawyers on behalf and behalf of their clients. To increase the efficiency of the registration procedure and create better conditions for electronic registration, this type of authorization was entrusted to lawyers.[2]

In Article 24 of the Law, the legislator stipulated that the delivery of the written notice of the registrar's decision is done at the request of the applicant, and for information, in alternative ways: by mail, by sending it to a registered address for receiving electronic mail, by picking it up at the headquarters of the Business Registers Agencyor its organizational parts. However, if an electronic application is submitted, the registrar's decision in electronic form is sent to the registered address for receiving electronic mail or to the address for receiving electronic mail indicated in the application. In addition to the above, to users of the electronic administration service registered by the Law regulating electronic administration, delivery is made exclusively to the Single electronic inbox.[3]

Harmonization of theCompanies Law was carried out in 2021, whereby according to Article 11, paragraph 3, it is prescribed that there is no obligation to certify the signature in a digitalized document, as it is replaced by a qualified electronic signature.

[2] Attorneys have the opportunity to certify digitalized documents from November 17, 2022.

[3] The implementation of the provisions related to submission to the Single Electronic Pad has been postponed to May 17, 2023.

Through the normative analysis of the Rulebook on Validation of Qualified Electronic Signatures and Qualified Electronic Seals, it was determined that the system used for validating a qualified electronic signature includes an installed validation application, within which validation is implemented and a management application through which the relying party initiates and obtains the status validation and validation report.

The Republic of Serbia has adopted the Capital Market Development Strategy for the period from 2021 to 2026 to increase the degree of competitiveness, efficiency, transparency of work, as well as market productivity to provide a range of products and services at the highest quality level. By creating a unique central database, the Republic of Serbia indirectly influenced the increase in attractiveness, accessibility, and education of economic participants in the market, strengthening the principles of efficiency and economy.

The development of IT is a way to reduce costs. The implementation of digital services would enable the reduction of operating costs and the increase of energy efficiency. Digitalization of business today is imperative and the benefits obtained from digitalization come as a multiple-return investment. The necessity of digitalization and modernization of work is reflected in maintaining competitiveness in the market. The empirical part of the research consists of the Business Registers Agency website content analysis. One of the benefits of registering business entities using digital technology is its economy. Of course, all applicants pay the registration fee, but electronic applicants pay 4,500.00 RSD, which includes the registration fee and publication of documents of importance for the establishment, as opposed to a regular application by submitting a paper form, where applicants only pay a fee in the amount of 4,900.00 RSD, without other externalities.

The Government of the Republic of Serbia for the period 2020-2023 adopted the Program for improving the position of the Republic of Serbia on the World Bank's ranking of business conditions – "Doing Business", which would result in the foreign capital attraction. According to the data of the Program, in the global ranking regarding the area of starting a business, the Republic of Serbia is currently in 73rd place, although it is only 10.70 points away from the ideal position. The goal of this program adoption is to improve the process of establishing a business company, as well as to standardize and reduce costs in the process. In the aforementioned attachment, the Republic of Serbia adopted an Action Plan for improving its position. According to the Action Plan, changes were made to the Identity Card Law, whereby the Legislator legislated that the electronically qualified certificate is an integral

part of the identity card (ID). Therefore, when issuing an ID card, a qualified electronic signature is also issued at the same time, because the keys required for the electronic signature are integrated into the chip of the ID card.

Through empirical research, it was observed that the Agency regularly updates all regulations, by-laws, and instructions on individual procedures related to its business on its website. Foremore, prescribed forms are regularly published and updated, based on which online registration and record-keeping procedures are initiated. In support of what has been said, on their website you can find the most adequate examples of acts that can be models for creating the documentation needed for the registration process.

The advantage of database digitalization contributed to the fulfillment of the publicity principle and the availability of data and documents from the register. The Agency, as the owner of the software used to manage the registers, has enabled free access to data from the register, both to users and to third parties, through public data search.

The agency collects information about users, such as the domain name, IP address, and URL address from which the Business Registers Agencywebsite was accessed, as well as the date and time of access to the website. Also, the right of the Agency is to monitor all traffic on the network to identify unauthorized attempts to change the content on the site as well as other illegal activities. The Agency must prevent any kind of abuse in the use of the site and the denunciation of information during the registration of business entities and take care of security protection, integrity, and functionality of databases.

The research showed that it is necessary to ensure the public availability of official records of issued permits and other acts, which are a prerequisite for registration. Above all, it is necessary to provide Business Registers Agencywith access to criminal records and records kept by tax authorities.

4. Discussion

The fundamental basis of the successful operation of the world economy and business entities is the stability and certainty of global, regional, and local markets. Without business stability and security, world and regional economies, as well as market participants, cannot operate progressively and successfully (Mirković & Stojšić Dabetić, 2020, p. 55). The period of registration of business entities is identified with the new phase of the technological revolution, equating its importance with the emergence of the Internet (Goforth, 2021). The development of the Internet, which provides the basis for the emergence and development of electronic business, enables access

to relevant information in different digital forms in the business function of all economic users (Skorup, Krstić& Cogoljević, 2013). There is an aspiration to shape the Internet in the form of a unique and open platform for its users, which is of particular importance for economic entities, to achieve economic development and social progress.

The term digitalization implies the mass use of IT, communication, and all types of electronic commerce (Jašarević, 2016, p. 1104). The incremental changes brought about by digitalization have created opportunities for economic growth, but they will inevitably cause economic dislocation. The anticipated effect of digitalization will redefine many roles and business processes, which will change the dynamics in many processes, which will consequently lead to the expansion of new markets.

The exponential speed of development, the disruption in all major industries, and the pervasive impact on production and management systems are what distinguish this development from the previous industrial revolution. Despite all the advantages, the digital revolution also carries certain risks. With adequate guidance, it has the potential to spur innovation on a global scale (World Economic Forum, 2016). Information and communication technologies(ICT) are the backbone of this revolution, whose continuous development directly affects economic changes. Economic and political imperatives combine with technological innovation to fuel the growth of the digital economy (Bukht & Heeks, 2017, p. 20).

The digital economy, as an economy that functions primarily through digital technology, influenced the creation of the concept of digital business transformation (Kahrović, 2021, p. 141). Digitalization involves a key transformation of business and affects processes and organizational structures. Society as a whole is faced with accelerated and radical changes caused by the maturation of digital technologies and their penetration into the market. The transcendence of the digital economy creates space for the successful performance of business operations without the obligation of physical presence. The convergence of digitalization and liberalization of economic policy has provided a foundation for companies to provide their services while locations are scattered around the world, thus providing an opportunity for the development of local markets.

Rapid access to information on a global level is made possible by the application of digital technology, which transforms business methods and opens new spaces for the creation of new value (Pitić, Savić & Verbić, 2018, p. 108). Digital technology is not only manifested through individual IT artifacts (such as computers, software applications, mobile phones, etc.), but it also fits

into most other artifacts. Therefore, it results in a world imbued with digital technology (Stolterman & Fors, 2004, p. 689). Digital transformation is a vital topic for companies around the world. It usually involves discussions around advanced analytics, social networks, mobile telecommunications, or similar phenomena. Digital transformation affects business architecture in all areas, which makes business model (re)design vitally important, requiring business leaders to take a systematic approach in this direction (Blaschke, Cigaina, Riss & Shoshan, 2016).

The world has become digital, and so has the economy. In this context, the transformation of the linear economy into a circular economy is needed to increase the sustainability of the digital sector (Stojanović, 2021). The digital economy as a way of doing business uses ICT and the Internet with the use of knowledge from the following fields: economics, informatics, telecommunications, computing, and digital electronics (Spalević, Vićentijević & Ateljević, 2018, p. 30). ICT is considered a vital segment that pervades all spheres of economic activity, erasing national borders (Petrović, 2018). The digital transformation of the economy has led to the creation of new business models, new products, services, and new ways of doing business. Thus, the digital economy is growing at an accelerated pace and is expected to continue to do so in the coming years. An integral component of every society is the economy, which requires a higher degree of compatibility with digital technologies (Dukić Mijatović & Mirković, 2022).

The digital economy is the result of the modification of information and communication technology, which contributed to technologies becoming cheaper and widely standardized, innovating business processes and encouraging innovation in all sectors of the economy (OECD, 2015). The core of the digital economy is hyperconnectivity, which means the growing interconnectedness of people, organizations, and machines resulting from the Internet, mobile technology, and the Internet, while the direction of the digital economy is inclusive.

Globalization is a phenomenon that has provided countless advantages for businessmen and the development of their businesses, but also caused the acceleration of competition, as a result of which companies have difficulty achieving, maintaining, and improving their competitiveness in the market (Bakator, Đorđević, Ćoćkalo, Ćeha & Bogetić, 2021). The use of digital technologies requires a change in the way business entities operate, while at the same time strengthening the competitive position based on knowledge and innovation (Savić, Lazarević, Kukić & Marinković, 2019). Digitalization of company law is necessary, which integrates the use of digital technologies

in the domain of establishment and registration of business entities up to the deletion of a business from the Business Registers Agency(Vujisić, 2019).

By enacting amendments to the Law on the Procedure of Registration in the Business Registers Agency and implementing amendments to other relevant laws in the field of electronic signatures, the Republic of Serbia carried out a curricular reform. Perceiving the Law, the changes aim to reduce the time spent, but also the costs required for the establishment of economic entities, to improve the conditions for starting a business, as well as the necessity of removing legal gaps observed in the application of regulations so far, and following the measures from the Action Plan of the Program for the Improvement of the Position of the Republic of Serbia in the ranking list of the World Bank on business conditions – "Doing Business" for the period 2020-2023.

5. Conclusion

The digitalization process represents a global trend that is perpetuated. Accordingly, it manifests itself as a necessary precondition for the survival of companies in the domestic and world markets. Its influence is reflected in the modernization of the economy, providing enormous opportunities, but also significant challenges for corporate management of companies. The concept of digitalization implies the continuity of cooperation and coordination between entities. By implementing the establishment of a digitalized procedure for the registration of business entities, an interactive record of business entities was created, which increased the agility of further development. The state must invest time and resources of all kinds to implement a digital culture. In all spheres of business, digitalization has enabled accelerated economic growth and development, economic efficiency, competitiveness, and profitability, thanks to the digitalization implementation and electronic connection of business entities, public administration bodies, and citizens. The legislator's motive for the aforementioned amendments is to save time and reduce the costs of establishing business entities, as well as the continuation of the digitalization of the Business Registers Agency and administration as a whole. Digitalization certainly represents a catalyst for innovation, modernization, and economic prosperity of the state. Successful digital transformation through the development of electronic services of a high level of sophistication is possible with a legal basis in the legislation, which predestined the reform in the domain of the concise legislative framework governing this area. The discourse analysis of this issue refers to the provisions of the Law on the Procedure of Registrationin the Business

Registers Agency, especially the changes that will take place next year, and they refer to the possibility of electronic registration of all business entities, which was not the case until now. The Agency represents a representative example of good practice in the organization of public administration, whose work is harmonized with the most modern digital technologies. The research concluded that the operational implementation of digital technologies is still necessary, as well as the building of both internal and external knowledge in the work of Business Registers Agencyon regulating the registration of business entities to further modernize business processes, strengthen the service function, and simplify administrative procedures.

Conflict of interests
The authors declare no conflict of interests.

Vasić Milica
Pravni fakultet za privredu i pravosuđe u Novom Sadu, Univerzitet Privredna akademija u Novom Sadu, Srbija

Bulatović Petar
Poslovno-umetnička akademija primenjenih studija u Beogradu, Srbija

DIGITALNA TRANSFORMACIJA AGENCIJE ZA PRIVREDNE REGISTRE U FUNKCIJI SAVREMENOG DIGITALNOG DRUŠTVA

REZIME: Digitalizacija snažno utiče na privredu i društvo u celini u različitim dimenzijama. Proces digitalizacije Agencije za privredne registre, kao i postupak registracije privrednih subjekata predstavlja jedan od prioritetnih zadataka koji ima za cilj povećanje efikasnosti i ekonomičnosti, kao i prosperitet privrede uopšte. Svakako da je preduslov postojanje digitalne pismenosti, koja nije izolovana kategorija, već nadgradnja ranijih oblika pismenosti. Nepobitno je da svaka inovacija nastaje kao privilegija viših društvenih slojeva, koja se po inerciji pretvara u potrebu ostalih. U ovom radu je analiziran legislativni okvir elektronske registracije privrednih subjekata. Polazeći od stava da je ekonomski rast, konkurentnost na tržištu, društveno-

ekonomski razvoj nužnost današnjice, autori kroz ovaj rad prevashodno nastoje da definišu ostvareni napredak rada Agencije za privredne registre pri registrovanju privrednih subjekata u procesu digitalizacije. Kvintesencija ovog rada jeste identifikacija dostupnosti digitalnih alata za registraciju privrednih subjekata, kao i njihova kvantifikacija i kvalifikacija.

Ključne reči: *Digitalno društvo, Agencija za privredne registre, registracija, digitalna ekonomija.*

References

1. Bakator, M., Đorđević, D., Ćoćkalo, D., Ćeha, M. & Bogetić, S. (2021). CRM i podaci korisnika – izazovi poslovanja u digitalnoj ekonomiji [CRM and user data – business challenges in the digital economy]. *Journal of Engineering Management and Competitiveness* (JEMC), *11*(2), pp. 85-95
2. Blaschke M., Cigaina M., Riss U.V. & Shoshan I., (2017). Designing Business Models for the Digital Economy. Shaping the Digital Enterprise: Trends and Use Cases in Digital Innovation and Transformation, *Springer International Publishing*, pp. 121-136, DOI: 10.1007/978-3-319-40967-2_6
3. Bukht R.& Heeks R., (2017). Defining, Conceptualising and Measuring the Digital Economy, Development Informatics, Working paper, No 68, *Centre for Development Informatics Global Development Institute*, SEED University of Manchester, Manchester, UK
4. Directive (EU) 2019/1151 of the European Parliament and of the Council of 20 June 2019 amending Directive (EU) 2017/1132 as regards the use of digital tools and processes in company law (Text with EEA relevance).Downloaded 2022, November 11 from https://eur-lex.europa.eu/eli/dir/2019/1151/oj
5. Dukić Mijatović, M. & Mirković, P. (2022). Digitalna ekonomija i informaciono društvo – domet i pristup pravne regulacije [Digital economy and information society – scope and approach of legal regulation].*Ekonomija – teorija i praksa,11*(2), pp. 53-70
6. Goforth, C., (2021).Regulation of Crypto Who Is the Securities and Exchange Commission Protecting?, *American Business Law Journal*, *58*(3), pp. 643-644
7. Jašarević, S. R. (2016). Uticaj digitalizacije na radne odnose [The impact of digitalization on labor relations]. *Zbornik radova Pravnog fakulteta*, *Novi Sad, 50*(4), pp. 1103-1117

8. Kahrović, E. (2021). Uticaj digitalne transformacije poslovanja na formulisanje novih korporativnih strategijskih pravaca [The impact of digital business transformation on the formulation of new corporate strategic directions]. *Naučne publikacije Državnog univerziteta u Novom Pazaru*. Serija B, *Društvene i humanističke nauke, 4*(2), pp. 141-153
9. Mirković, P. & Stojšić Dabetić, J. (2020). Alternativni načini organizovanja privrednog poslovanja za vreme pandemije Covid 19 – izazovi elektronske trgovine [Alternative ways of organizing business operations during the Covid 19 pandemic – challenges of electronic commerce]. *Kultura polisa*, *17*(2), pp. 55-68.
10. Odluka o naknadama za poslove registracije i druge usluge koje pruža Agencija za privredne registre [Decision on fees for registration and other services provided by the Business Registers Agency]. *Službeni glasnik RS*, br. 119/13, 138/14, 45/15, 106/15, 32/16, 6950/16, 75/18, 73/19, 15/20, 91/20, 11/21, 66/21 i 129/21
11. OECD (2015). Adressing the Tax Challenges of the Digital Economy, Action 1 – 2015 Final Report, OECD G20 BEPS Project, OECD Publishing, Paris.https://doi.org/10.1787/9789264241046-en
12. Petrović, D. (2018). Primena koncepta elektronske trgovine u Srbiji [Application of the electronic commerce concept in Serbia]. *Vojno delo*, 70(7), pp. 423-430
13. Pitić, G., Savić, N.& Verbić, S. (2018). Digitalna transformacija i Srbija [Digital transformation and Serbia]. *Ekonomika preduzeća, 66*(1-2), pp. 107-119
14. Pravilnik o validaciji kvalifikovanog elektronskog potpisa i kvalifikovanog elektronskog pečata [Rulebook on Validation of Qualified Electronic Signature and Qualified Electronic Seal]. *Službeni glasnik RS*, br. 43/19
15. Program za unapređenje pozicije Republike Srbije na rang-listi Svetske banke o uslovima poslovanja – "Doing business" za period 2020–2023. godine [Program for improving the position of the Republic of Serbia on the World Bank's ranking of business conditions – "Doing Business" for the period 2020 – 2023]. *Službeni glasnik RS*, br. 89/20-143
16. Savić, N., Lazarević, J., Kukić, Z.& Marinković, E. (2019). Digitalna transformacija – izazovi kompanija u Srbiji [Digital transformation – challenges of companies in Serbia]. *Ekonomika preduzeća*, 67(1-2), pp. 101-114
17. Skorup, A., Krstić, M.& Cogoljević, M. (2013). Trendovi e-poslovanja u uslužnoj delatnosti [E-business trends in the service industry]. *Trendovi u poslovanju*, *1*(1), pp. 97-108

18. Spalević, Ž., Vićentijević, K. & Ateljević, M. (2018). Pravno-ekonomska analiza stepena razvoja digitalne ekonomije [Legal and economic analysis of the digital economy development level]. *Trendovi u poslovanju, 6*(1), pp. 29-37
19. Stojanović N., (2021). Evropski zeleni dogovor – put ka zelenoj i digitalnoj transformaciji privrede i društva Evropske unije [The European Green Deal – the path to a green and digital transformation of the economy and European Union society]. *Pravo i digitalizacija*: *zbornik radova: međunarodna naučna konferencija*[*Law and digitalization: proceedings: international scientific conference*] (pp. 149-160), Niš: Univerzitet u Nišu, Pravni fakultet
20. Stolterman, E.& Fors, A.C. (2004). Information Technology and the Good Life. in: Kaplan, B., Truex, D.P., Wastell, D., Wood-Harper, A.T., DeGross, J.I. (eds.), *Information Systems Research: IFIP International Federation for Information Processing* (pp. 687–692). Boston:Springer
21. Strategija za razvoj tržišta kapitala za period od 2021. do 2026. godine [Capital market development strategy for the period from 2021 to 2026]. *Službeni glasnik RS*, br. 102/21
22. Vujisić, D. (2019). Digitalizacija kompanijskog prava [Company law digitalization]. *Pravo i privreda*, *57*(4-6), pp. 144-153
23. World Economic Forum, The Global Information Technology Report, Geneva, 2016. Downloaded 2022 November7,from https://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf
24. Zakon o elektronskom dokumentu, elektronskoj identifikaciji i uslugama od poverenja u elektronskom poslovanju [Law on Electronic Document, Electronic Identification and Trust Services in Electronic Business]. *Službeni glasnik RS*, br. 94/17 i 52/21
25. Zakon o izmenama i dopunama Zakona o postupku registracije u Agenciji za privredne registre [Law on Amendments to the Law on the Procedure of Registration in the Business Registers Agency]. *Službeni glasnik RS*, br. 105/21
26. Zakon o postupku registracije u Agenciji za privredne registre [Law on the Procedure of Registration in the Business Registers Agency]. *Službeni glasnik RS*, br. 99/11, 83/14, 31/19 i 105/21
27. Zakon o privrednim društvima [Companies Law]. *Službeni glasnik RS*,br. 36/11, 99/11, 83/14 – dr. zakon, 5/15, 44/18, 95/18, 91/19 i 109/21

THE INSTRUCTION TO THE AUTHORS
FOR WRITING AND PREPARING MANUSCRIPTS

The Editorial board of the "Law - theory and practice" journal asks the authors to write their manuscripts to be published according to the following instruction.

In the journal there are being published the pieces of work referring to legal, economic and social disciplines. Namely, in the journal there are published: scientific articles, surveys, reviews, the analyses of regulations, the comments on the court decisions, students' papers and other additional texts. The manuscripts are to be sent in English through OJS online platform.(http://casopis.pravni-fakultet.edu.rs/index.php/ltp/about/submissions)

All manuscripts must submit to review. Each scientific paper must be reviewed by at least two reviewers according to the choice of the editorial board.

The editorial board has the right to adjust the manuscript to the editorial rules of the journal.

General information about writing the manuscript:

The manuscript should be written in the Microsoft Word text processor, Times New Roman font of the value of 12 pt, in Latin letters, with a spacing of 1,5. One is supposed to use the value of 25 mm for all margins. The scope of the manuscript can be of 12 pages at most in an A4 format including a text, tables, pictures, graphs, literature and other additional material.

The title-page of the paper should contain the title of the paper work in English, and below it there should be written the same thing in Serbian of the font size of 14 pt, Bold. After that, there is a spacing and, then, there should be stated the author's name and surname, his/her title, affiliation (the work place **with obligatory stating the name of the country too)**, an e-mail address and contact phone, the font size of 12 pt. If the author has his/her ORCID number, it should be stated immediately after his/her name and surname. For more information about ORCID iD, please visit https://orcid.org and after the registration insert your ORCID iD number.

Then, there is a spacing, and after that there should be written an abstract of the length to 250 words in English, and in Serbian below it of

the font size of 12 pt. An abstract represents a brief informative contents review of the article enabling the reader's quick and precise judgment of its relevance. The authors have to explain the goal of their research or to state the reason why they decided to write the article. Then, it is needed the methods being used in a research to be described including a short description of the results being reached in a research.

Key words are stated after one line of a spacing below the abstract written in English, and, also, in Serbian below it. There should maximally be five of them, of the font size of 12 pt, Italic. Then comes a two-line spacing and the text of the paper work.

Manuscript should be written concisely and intelligibly in a logical order which, according to the rule, includes the following: an introduction, the working out of the topic and a conclusion. The letters of the basic text should be of the font size of 12 pt. Titles and subtitles in the text are supposed to be of the font size of 12 pt, Bold.

The name and number of illustrations (diagrams, photographs, graphs) should be represented in the middle of the line above the illustration, the font size of 12 pt. The name and number of a table should also be represented in the middle of the line above the table, the font size of 12 pt. Below the illustration or table, it is obligatory the source to be stated ("Source:…"), the font size of 10 pt. If the results of the author's research are represented in the form of a graph or table, there should be stated as a source below the illustration or table: Author's research.

If the author of the text writes a thank-you note or states the project references within which the text has been written and the like, he/she does it in a special section – Acknowledgments, which, according to the ordinal number, comes after the Conclusion, and before the author's affiliation and the summery of the text written in Serbian.

Use APA style to write references (The hand book for publishing, the American Psychological Association) as an international standard for writing references. Remarks, namely footnotes, may contain additional explanations or comments referring to the text. Footnotes are written in a font size of 10 pt.

Within the APA style, the used source is stated **inside the text,** in the way the elements (the author, the year of publication, the page number where the quoted part is) are indicated in parentheses immediately before the full stop and separated by a comma.

Citing rules inside the manuscript

If the cited source has been written by one author:

When a sentence contains the author's name and his/her cited words, then, after the author's name, there is stated the year of publication of the cited text in the brackets. At the end of the sentence, it is necessary the page number on which there is a sentence from the cited text to be indicated:

There is an example:

As Besermenji (2007) points out, "it is especially present the problem of the air pollution, which is explicitly a consequence of an extremely low level of ecological awareness as well as the lack of professional education in the field of environment" (p. 496).

In the case when the author is not mentioned in the sentence, his/her surname, the year of publication of the paper work and the page number in the paper should be put in brackets and at the end of the sentence.

There is an example:

Also, "rural tourism is expected to act as one of the tools for sustainable rural development" (Ivolga, 2014, p. 331).

A note: If a citation has been made by paraphrasing or resuming, then it is not necessary the page number to be stated.

There is an example:

The environment represents everything that surrounds us, namely everything with which a human's living and producing activity is either directly or indirectly connected (Hamidović, 2012).

If the cited source has been written by two authors:

There should be put "and" or "&" between the authors' surnames depending on the fact whether the authors are mentioned in the sentence or not.

There are some examples:

Chaudhry and Gupta (2010) state that as many as 75% of the world's poor live in the rural areas and more than one-third of rural areas are in arid and semiarid regions.

Hence, "rural development is considered as a complex mesh of networks in which resources are mobilized and in which the control of the process consists of interplay between local and external forces" (Papić & Bogdanov, 2015, p. 1080).

If the cited source has been written by three to five authors:

When such a source is cited for the first time, all the authors should be stated:

There is an example:

(Cvijanović, Matijašević Obradović & Škorić, 2017)

When this source is later cited again, there should be stated only the first author's surname and added "et al.".

There is an example:

(Cvijanović et al., 2017)

If the cited source has been written by six and more authors:

By the first and all further citations, the first author's surname should be stated and added "et al.".

There is an example:

(Savić et al., 2010)

If the author of the cited text is an organization:

In the case when the author of the cited text is an organization, then its name should be put in brackets as an author of the text. If the organization has a known abbreviated name, then one has to write this abbreviated name in a square bracket, after the full name, in the first citation, while any further citation should be marked by this abbreviated name.

There is an example:

the first citation: (Serbian Academy of Sciences and Arts [SASA], 2014)

further citations: (SASA, 2014)

If the authors of the cited text have the same surname:

In the case of the authors having the same surname, there should be used the initials of their names in order to avoid the confusion.

There is an example:

The attitude made by D. Savić (2017) is presented...

If there are cited several references of the same author from the same year:

If there are two or more references cited from the same author and from the same year, then, after the fact of the year, there have to be added the marks "a", "b", etc.

There is an example:
(Dragojlović, 2018a)
(Dragojlović, 2018b)

If there exist two or more texts in one citation:

When one cites two or more texts in one citation, then, in brackets, there are stated the surnames of the authors of original texts in the order of publication and they are separated by a semicolon.

There is an example:

Obviously, living and working in rural areas has always been connected with specific material and symbolical relations to nature (Milbourne, 2003; Castree & Braun, 2006).

If there is cited the newspaper article with the stated author:

There is an example:

In *NS uživo* there was published (Dragojlović, 2021) that...

In the list of the used references, this reference should be written in the following way: Dragojlović, J. (2021). Anketirani Novosađani za vraćanje smrtne kazne u Ustav [Novi Sad residents surveyed to return the death penalty to the Constitution]. *NS uživo*, January 22.

If there is cited the newspaper article without the author being stated:

There is an example:

Published in *Politika* (2012)

In the list of the used references, this reference should be written in the following way: *Politika*. (2012). Straževica gotova za dva meseca [Straževica finished in two months]. February 1.

If the personal correspondence is cited:

The example: According to Nikolić's claims (2020),

In the list of the used references, this reference should be written in the following way: Nikolić, A. (2020). Pismo autoru [Letter to the author], 21. novembar.

If it is cited the text in press, at the end of the reference, and before the full stop, it is obligatory to add "in press".

If the court decisions, the praxis of the European court for human rights, and other sources from both national and international court praxis are cited, a reference should contain as much precise facts as it is possible: the type and number of the decision, the date when it was made, the publication where it was published.

The example in the text: (The Decision of the Superior court in Belgrade - A special department K.Po1 no. 276/10 from 26th January 2012)

The example in the text: (Borodin v Russia, par. 166.)

A note:

The sources from the court praxis **are not stated** in the list of the used literature. A full reference from the court praxis **is stated** in a footnote. While citing the European court for human rights praxis there should be indicated the number of the submitted petition.

There is an example of a reference in a footnote:

As it is stated in the Decision of the Superior court in Belgrade - A special department K.Po1 no. 276/10 from 26th January 2012 Intermex (2012). Bilten Višeg suda u Beogradu [Bulletin of the High Court in Belgrade], 87, p. 47.

Borodin v Russia, the petition no. 41867/04, the sentence ECHR, 6. 2. 2013, par. 166.

If the laws and other regulations are cited:

When citing a legal text or other regulation, in the text there should be stated a full name of law or other regulation including the year when the law or regulation was enforced.

There is an example:

(The Code of criminal procedure, 2011)

(The Book of rules on the content of the decision on conducting the procedure of public procurement made by several consignees, 2015)

This rule is also applied to laws and other regulations not being in force any longer.

There is an example:

(The Criminal law act of Republic of Serbia, 1977)

When citing the international regulations, in the text it is enough to state a shortened name of the document together with its number and year when it was accepted.

There is an example:

(Regulation No. 1052/2013) ili (Directive 2013/32)

If there is cited the text of the unknown year of publication or the unknown author's paper work:

In the paper work, such a kind of text should be cited in the way that in the place of the year there is stated "n.d." (non dated).

There is an example:

Their significance for parliamentary processes is unmeasureable (Ostrogorski, n.d.).

If there is a paper work of the unknown author used in a manuscript, there will be stated the title of the paper being cited together with the year, if it is known.

There is an example:

All these are confirmed by a mixed, objective-subjective theory (The elements of a criminal offense, 1986, p. 13).

An important note:

The cited sources (regardless the fact in which language they have been written) are not supposed to be translated into English, except the title of the paper work (publications, a legal act or bylaw) which should be translated and written in a square bracket.

The example:

1.) Matijašević Obradović, J. (2017). Značaj zaštite životne sredine za razvoj ekoturizma u Srbiji [The importance of environmental protection for the development of ecotourism in Serbia]. *Agroekonomika*, *46* (75), pp. 21-30.

2.) Jovašević, D. (2017). *Krivična dela ubistva* [*Murder as a Crime*]. Beograd: Institut za kriminološka i sociološka istraživanja.

3.) Uredba o ekološkoj mreži Vlade Republike Srbije [The Ecological Network Decree of the Government of the Republic of Serbia]. *Službeni glasnik RS*, no. 102/10

4.) Zakon o turizmu [The Law on Tourism]. *Službeni glasnik RS*, no. 17/19

At the end of each text, in the section under the name of "**References**", it is obligatory to state the list of all cited references according to an alphabetical order. The titles in foreign languages beginning with definite or indefinite articles ("a", "the", "Die", ...) are ordered as if the article does not exist. The reference list should only include the works that have been published or accepted for publication.

The editorial board insists on the references of recent date, which will specially be taken into account while choosing the manuscripts to be published. At the end of each reference, it is obligatory to state a DOI number, if the cited reference contains it. If the cited reference does not contain a DOI number, the author can refer to the URL address.

The example of the stated reference together with a DOI number:

Počuča M., & Matijašević Obradović, J. (2018). The Importance of Evidence Collection in Procedures for Criminal Acts in the Field of Economic Crime in Serbia. In: Meško, G., et al. (eds.), *Criminal Justice and Security in Central and Eastern Europe: From Common Sense to Evidence-based Policy-making* (pp. 671-681). Maribor: Faculty of Criminal Justice and Security and University of Maribor Press. DOI: 10.18690/978-961-286-174-2

The example of the stated reference together with an URL address:

Milosavljević, B. (2015). Pravni okvir i praksa primene posebnih postupaka i mera za tajno prikupljanje podataka u Republici Srbiji [Legal framework and practice of application of special procedures and measures for secret data collection in the Republic of Serbia]. In: Petrović, P. (ured.), *Posebne mere tajnog prikupljanja podataka: između zakona i sudske prakse* [*Special measures for secret data collection: between law and case law*] (pp. 5-33). Beograd: Beogradski centar za bezbednosnu politiku. Downloaded 2021, January 15 from https://bezbednost.org/wp-content/uploads/2020/06/posebne_mere_tajnog_prikupljanja_podataka_-_vodic_.pdf

The examples of the used references being stated at the end of the paper work:

References:

1. Agencija za privredne registre. *Privredna društva* [*Companies*]. Downloaded 2020, January 10 from https://www.apr.gov.rs/o-agenciji.1902.html
2. *California Secretary of State*. Downloaded 2020, December 15 from https://www.sos.ca.gov/business-programs/
3. Dukić-Mijatović, M. (2011). Korporativno upravljanje i kompanijsko pravo Republike Srbije [Corporate Governance and Companies Business Law of the Republic of Serbia]. *Pravo -teorija i praksa*, *28* (1-3), pp. 15-22.
4. Dragojlović, J., & Bingulac, N. (2019). *Penologija između teorije i prakse* [*Penology between theory and practice*]. Novi Sad: Pravni fakultet za privredu i pravosuđe u Novom Sadu.
5. Dragojlović, J. (2021). Anketirani Novosađani za vraćanje smrtne kazne u Ustav [Novi Sad residents surveyed to return the death penalty to the Constitution]. *NS uživo*, January 22.
6. Gopalsamy, N. (2016). *A Guide to Corporate Governance*. New Delhi: New Age International.
7. Jesover, F., & Kirkpatrick, G. (2005). The Revised OECD Principles of Corporate Governance and their Relevance to Non-OECD Countries. *Corporate Governance: An International Review*, *13* (2), pp. 127-136. DOI: 10.1111/j.1467-8683.2005.00412.x
8. Milosavljević, B. (2015). Pravni okvir i praksa primene posebnih postupaka i mera za tajno prikupljanje podataka u Republici Srbiji [Legal framework and practice of application of special procedures and measures for secret data collection in the Republic of Serbia]. In: Petrović, P. (ured.), *Posebne mere tajnog prikupljanja podataka: između zakona i sudske prakse* [*Special measures for secret data collection: between law and case law*] (pp. 5-33). Beograd: Beogradski centar za bezbednosnu politiku. Downloaded 2021, January 15 from https://bezbednost.org/wp-content/uploads/2020/06/posebne_mere_tajnog_prikupljanja_podataka_-_vodic_.pdf
9. Počuča M., & Matijašević Obradović, J. (2018). The Importance of Evidence Collection in Procedures for Criminal Acts in the Field of Economic Crime in Serbia. In: Meško, G., et al. (eds.), *Criminal Justice and Security in Central and Eastern Europe: From Common Sense to Evidence-based Policy-making* (pp. 671-681). Maribor: Faculty of

Criminal Justice and Security and University of Maribor Press. DOI: 10.18690/978-961-286-174-2
10. Regulation (EU) No. 1052/2013 establishing the European Border Surveillance System (Eurosur), OJ L 295 of 6/11/2013.
11. Škorić, S. (2016). *Uticaj poslovnog imena privrednog društva na njegovo poslovanje - doktorska disertacija* [*The influence of the business name of the company on its business - doctoral thesis*]. Novi Sad: Pravni fakultet za privredu i pravosuđe u Novom Sadu.
12. Škulić, M. (2007). *Krivično procesno pravo* [*Criminal Procedural Law*]. Beograd: Pravni fakultet Univerziteta u Beogradu i JP Službeni glasnik.
13. Uredba o ekološkoj mreži Vlade Republike Srbije [The Ecological Network Decree of the Government of the Republic of Serbia]. *Službeni glasnik RS*, br. 102/10.
14. Veljković, N. (2017*). Indikatori održivog razvoja: Srbija i svet* [*Sustainable development indicators: Serbia and the world*]. Downloaded 2017, October 22 from http://indicator.sepa.gov.rs/o-indikatori
15. Zakonik o krivičnom postupku [Criminal Procedure Code]. *Službeni glasnik RS,* no. 72/11, 101/11, 121/12, 32/13, 45/13, 55/14 and 35/19.