JURNAL CITA HUKUM (Indonesian Law Journal)
FSH UIN Syarif Hidayatullah Jakarta
Vol. 10 No. 3 (2022), pp. 473- 482, DOI: 10.15408/jch.v10i3.26095

Application of Digital Technologies in Law*

Ludmila Grudtsina[1], Mehriban Elbrus kyzy Guliyeva[2], Sergei Zhdanov[3], Badma Sangadzhiev[4], Victor Shestak[5]

[1]North-West Institute (branch) of the University named after O.E. Kutafin (Moscow State University), [2]Financial University under the Government of the Russian Federation, [3]Plekhanov Russian University of Economics, [4]Peoples Friendship University of Russia (RUDN University), [5]Moscow Academy of the Investigative Committee of the Russian Federation, Russia

10.15408/jch.v10i3.26095

Abstract

The study's purpose is to examine the nature, concepts, and grounds for the use of various types of digital technologies in law, to concisely and clearly outline the systematized foundations of scientific knowledge on the application of digital technologies in regulation and legislation on the example of the Russian Federation, with the involvement of legislative practices of foreign countries. The deductive method was the primary method of the study, which allowed us to consider the nature and foundations, forms, and methods of using digital technologies in law and legislation. In addition, the inductive method, the practice of systemic scientific analysis, and comparative legal and historical methods were used. The top way underlying the solution to the issue is to study the legal foundations and features of using digital technologies in law. The study proves the unsolved theoretical problem of scientific understanding of the types and forms of application of digital technologies in law in the example of the Russian Federation and some countries of the world. The authors argue that digital technologies store much information, thereby simplifying the transaction system. It allows us to receive information quickly and, as a result, significantly save time and speed up the process of transferring data.

Keywords: Civil law; digital rights; digital technologies; human rights; international communications

* Received: May 14, 2022, Revised: June 21, 2022, Accepted: July 16, 2022, Published: December 30, 2022.

[1] **Ludmila Grudtsina** is a Professor at the North-West Institute (branch) of the University named after O.E. Kutafin (Moscow State University). https://orcid.org/0000-0001-7731-724X. Email: grudtsina.l.yu@mail.ru

[2] **Mehriban Elbrus kyzy Guliyeva** is a researcher at Financial University under the Government of the Russian Federation. https://orcid.org/0000-0002-6124-4880. Email: m.e.k.guliyeva@mail.ru

[3] **Sergei Zhdanov** is an Associate Professor at the Plekhanov Russian University of Economics. https://orcid.org/0000-0002-1330-8165. Email: zhdanov120009@yandex.ru

[4] **Badma Sangadzhiev** is a Professor at the Peoples Friendship University of Russia (RUDN University). https://orcid.org/0000-0001-8317-0117. Email: sangadzhiev-bv@rudn.ru

[5] **Victor Shestak** is an Associate Professor at the Moscow State Institute of International Relations (MGIMO) of the Ministry of Foreign Affairs of Russia. https://orcid.org/0000-0003-0903-8577. Email: viktor_shestak@mail.ru

*Corresponding Author: grudtsina.l.yu@mail.ru

Penerapan Teknologi Digital dalam Hukum

Abstrak
Tujuan studi ini adalah untuk mengkaji sifat, konsep, dan dasar penggunaan berbagai jenis teknologi digital dalam hukum, untuk menguraikan secara ringkas dan jelas landasan sistematis pengetahuan ilmiah tentang penerapan teknologi digital dalam hukum dan perundang-undangan. Misalnya Federasi Rusia, dengan keterlibatan praktik legislatif negara asing. Metode deduktif adalah metode utama penelitian yang memungkinkan untuk mempertimbangkan sifat dan dasar, bentuk, serta metode penggunaan teknologi digital dalam hukum dan perundang-undangan. Selain itu, metode induktif, metode analisis ilmiah sistemik, hukum komparatif dan sejarah digunakan. Metode utama yang mendasari penyelesaian masalah ini adalah mempelajari landasan hukum dan fitur penggunaan teknologi digital dalam hukum. Studi tersebut membuktikan masalah teoretis pemahaman ilmiah yang belum terpecahkan tentang jenis dan bentuk penerapan teknologi digital dalam hukum dengan contoh Federasi Rusia dan beberapa negara di dunia. Penulis berpendapat bahwa teknologi digital menyimpan sejumlah besar informasi, sehingga sangat menyederhanakan sistem transaksi. Hal ini memungkinkan untuk menerima informasi dengan cepat dan, sebagai hasilnya, secara signifikan menghemat waktu dan mempercepat proses transfer informasi.
Kata Kunci: Hukum perdata; hak digital; teknologi digital; hak asasi Manusia; komunikasi internasional.

Применение Цифровых Технологий В Праве

Абстрактный.
Цель статьи заключается в изучении природы, понятия и оснований применения различных видов цифровых технологий в праве, в том, чтобы кратко и доступно изложить систематизированные основы научных знаний по вопросам применения цифровых технологий в праве и законодательстве на примере Российской Федерации, с привлечением законодательных практик зарубежных стран. Методы. Основным методом исследования стал дедуктивный метод, позволивший рассмотреть сущность и основания, формы, а также способы использования цифровых технологий в праве и законодательстве. Кроме того, использовались индуктивный метод, метод системного научного анализа, сравнительно-правовой и исторический методы. Ведущий метод, заложенный в основу решения проблемы, состоит в изучении правовых основ и особенностей применения цифровых технологий в праве. Результаты. В исследовании доказывается теоретическая нерешенность проблемы научного осмысления видов и форм применения цифровых технологий в праве на примере Российской Федерации и некоторых стран мира. Авторы утверждают, что цифровые технологии хранят большой объем информации, тем самым значительно упрощая систему транзакций. Новшество позволяет оперативно получать информацию и как следствие, значительно экономит время и ускоряет процесс передачи информации.
Ключевые слова: гражданское право; цифровые права; цифровые технологии; права человека; международные коммуникации.

A. INTRODUCTION

The Internet is gradually becoming the environment where intellectual property rights violations are most common. Therefore, it is essential to find and maintain a balance of interests of all parties involved in order, on the one hand, to strengthen the fight against "piracy"; and, on the other, to improve cooperation between information intermediaries, rights holders, and regulators in the development of an effective mechanism for the protection of intellectual property on the Internet. Thus, it is hardly possible to call the "anti-piracy law" a threat to the development of the Internet in Russia. On the contrary, the legal regulation of this sphere of relations aims to limit the activities of unscrupulous entrepreneurs who make money on Internet piracy. Legal services will not be affected by it.

The monetization of the Internet space is taking place rapidly, and new objects of copyright appear, the main feature of which is the digital form. Thus, the owners of domains and e-mails are trying to retain the right to use a unique "address" and not concede it to the copyright holders of companies with the same commercial designation. Internet media owners specializing in creating applications and video games are losing tens of thousands of dollars in developing their information products due to illegally copying materials and posting them on other sites. Disputes are flaring up around the problem of providers' liability for unlawful actions of users, as well as the fact of the "anonymity" of the Internet (Galakhova, 2011). The main issue associated with protecting copyright violated in information networks is proving the illegal distribution of intellectual property objects. In the Russian doctrine and law enforcement practice, there are several points of view on what evidence should be presented to the court to confirm copyright infringement on the Internet.

B. METHODS

The deductive method was the primary method, which allowed us to consider the legal nature and features of using digital technologies in law. In addition, the inductive method, systemic scientific analysis, and comparative legal and historical approaches were used. Digital technologies store much information, thereby greatly simplifying the transaction system. It allows us to receive information quickly and, as a result, significantly save time and speed up the process of transferring data. Companies that use digital technologies become more competitive, reduce production costs, and therefore become more profitable, which generally leads to the development of the economy.

The development of digital technologies and their application to law and national legislation are written by such foreign authors as B. Barber (1984), D. Bell (1999), A. Chianale (1990), P. Drucker (1993), F. Fischer (1991), and A. Toffler (1990). In addition, several Russian scientists study the problems of the information environment and the impact of information technology on the law: V.V. Adrianov (2011), A.E. Galakhova (2011), L.Y. Grudtsina (2018), L.G. Yefimova (2017), I.V. Izmailov (2012), N.E. Tropynina (2020), etc. There were also quite a few experts who expressed concern about technocratization, especially during the global digital informatization period. In particular, F. Fischer and B. Barber write that technocratization undermines democracy to the extent that it pushes the population away from political participation, depriving the initiative of the bottom of meaning; it leads to the concentration of power in the hands of the elite, which manipulates public consciousness (Barber, 1982; Fischer, 1991). The concerns expressed are confirmed by modern practice, which demonstrates the lack of legal guarantees of protection against the abuse of "information power" by the technocracy.

C. RESULTS

Recently, in all countries, there has been a constant reform of the taxation system. Approaches to considering the tax system as performing not only a fiscal function but also a regulatory (stimulating) one are changing. Many countries have already resorted to changing the tax system to increase the level of innovation activity in the country (Ryan, 2008; Taranukha, 2020). Innovation activity is essential not only for enterprises within the government to increase the level of their competitiveness but also for the country as a whole because the level of innovative activity directly affects the economic and resource independence of one country from others and improves the quality of life of the population as well. At the moment, the formation of an innovative economy in Russia is not taking place, which does not allow for achieving the goals of improving the population's living standards and increasing the competitiveness of Russian products.

Conventionally, incentives for investment and innovation can be divided into direct investments from the state budget and tax incentives (Grudtsina et al., 2018). Today in Russia, several factors are slowing down the digitalisation process of enterprises. These include the lack of a well-built strategy, integration of new and existing technologies and data, outdated technologies, lack of close ties between IT and business, unwillingness to change, insufficient funding, management position, and possible risks. Due to the absence of clear boundaries on the protection of personal and user data in Russian legislation and the

inclusion of digital human rights in the Constitution of the Russian Federation, Internet users at the moment must take care of their security on the Internet: 1). Encryption of all data. Even if the computer system is protected with a password, an attacker can easily reset it by booting from an external drive. There is no need to reset the password either – any Live Linux distribution can easily read and copy the data. Therefore, one needs to take measures to encrypt information. 2). Using password managers, which generate new random passwords each time for any created account on the Internet. Absolute privacy on the Internet is impossible. However, the listed techniques can protect Internet users from fraudsters' theft of confidential data, the curiosity of colleagues sitting at the same table, and the annoying attention of Google and Microsoft marketers (Izmailov, Poizner, 2012).

D. DISCUSSION

Back in the 1990s and at the beginning of the 21st century, socio-philosophical concepts of technocratic appeared (D. Bell, E. Toffler, P. Drucker, M. Castells, etc.), substantiating the social and economic predetermination (historical inevitability) of the formation of a Technotronic society developing in digital information flows (Bell, 1999; Drucker, 1993; Toffler, 1990; Castells, 1996). History shows that technocratization is not fractal and has simultaneously generated positive and negative consequences (Schelsky, 1957; Marcuse, 2003; Habermas, 1979). The phenomenon of technocratization would not have been so pronounced in the modern era if it had not been for the development of information technology. This process is evaluated differently in contemporary science and social practice (Brzezinski, 1970; Galbraith, 1967; Rostow, 1960; Aron, 1994).

Is it possible to say that civil liability in providing services using digital technologies is interconnected with ethics (ethical norms) on the Internet and human rights in the digital environment? To the authors, these are interrelated concepts and phenomena. The largest European meeting on ethics and human rights in the information society was held in Strasbourg in September 2007. The meeting analyzed the opportunities offered by information technologies on the Internet and their side effects, adverse impact, and possible conflicts of interest. Recommendations have been made for a participatory and shared responsibility Internet governance model. The Internet governance model seems to presuppose a system of mechanisms, including legal ones, regulating the provision of services in the digital environment and bringing civil liability in providing services using digital technologies. (Shevchenko, Ivanova, Grudtsina, 2019)

Regional Info-ethics Meetings 2007-2010 within UNESCO laid the foundations for follow-up and initiated work on a *Code of Ethics for the Information Society*. During the 15th meeting in February 2009, the Bureau of the Information for All Program decided to prepare a draft of this document. The work was led by Karol Jakubowicz, who was then Chairman of the Intergovernmental Council of the Program.

The general human rights framework and the relevant studies of the Universal Declaration of Human Rights provided the starting points for formulating ethical norms and standards in the context of the information society. The Liability section included the Security, Legal Protection, Intellectual Property Rights, and Service Provider Liability subsections. The proposed draft Code was widely discussed at the 6th session of the Intergovernmental Council in March 2010 with the participation of 24 members of the Intergovernmental Council and representatives of member states who attended as observers. However, the lengthy 14-page document attempted to cover many topics at a very high level of detail. For this reason, the Intergovernmental Council asked the Program Office to continue working on the document and prepare a revised version. The Bureau entrusted this task to the representatives of Latvia and Venezuela.

The Code considers the interests of all member states and is not binding. It addresses all interested parties and defines the universal values and principles that should be observed when working with information and informed decision-making in the information society (including in the case of the offensive and bringing to civil liability). The document does not provide detailed guidance on specific actions. Still, it postulates basic ethical principles and values of the information society to give all members of the information society a suitable vector for action and decision-making. The Intergovernmental Council of the Information for All Program presented the *Code of Ethics for the Information Society* for approval at the 36th Session of the General Conference of UNESCO. Several Member States openly expressed deep satisfaction with the General Conference's sincere support of the Code. It noted the contribution of this document to the consideration of critical issues, the flexibility provided by its optional status, and the significant amount of advisory work during the preparation of this document. (Singer, 1993; Tropynina, Nikitina, 2019; Beliaeva et al., 2017)

After extensive discussion, it became clear that the positions and interests of the Member States are too contradictory and do not allow for an agreement. It seems that the Internet is such a powerful tool that some experts do not want to be constrained by ethical norms in using these tools. In contrast, others are

concerned about the possible use of ethics as an excuse to restrict such fundamental human rights as freedom of expression. A heated debate led to the decision to take note of the Code and to ask the Director-General for suggestions on how UNESCO could further work on ethical issues of relevance to the Information Society. Based on this experience, the Information for All Program consulted with Member States and other stakeholders. As a result, a document entitled *UNESCO and the Ethical Dimensions of the Information Society* was developed. The Executive Board of UNESCO, at its 190th Session in October 2012, adopted this document and proposals calling for action in the following directions: to build multi-stakeholder partnerships, raise awareness of the ethical dimensions of the information society and improve the effectiveness of action in this area; participate in international discussions on the ethical aspects of access to and use of information. The consequence of this decision was identifying the listed areas as priorities for further actions of the IFAP Working Group on info-ethics. Furthermore, as part of the WSIS +10 survey, a study *entitled Ethical and Societal Challenges of the Information Society* was prepared. It is based on *Ethical Implications of Emerging Technologies: A Survey* published by the Information for All Program in 2007.

It seems important to determine the limits of awareness of the violation of law in the provision of services in the digital space. The criterion of valid knowledge can be considered as the fact that the intermediary has specific and detailed information received from the copyright holder about the presence of a violation of the right. Assumed knowledge in domestic and foreign legislation is disclosed in different ways. In the article, the authors considered three possible situations: 1) when there is a court decision obliging to remove (delete) certain content, 2) there is only a statement by the copyright holder, 3) there is neither a statement nor a court decision, but it is possible to find out about the violation from other sources. In the first case, the intermediary must and can find out about violating the right in the event of repeated illegal posting of the copyright holder's material (Grudtsina, Galushkin, 2013). Thus, they become obliged to remove the content immediately. Otherwise, liability for copyright infringement may be placed on the intermediary. In the second case, the intermediary is also obliged to delete the materials of the copyright holder if they have sufficient data on the violation of the right. In the third case, it is necessary to apply the approach of the European Court and establish the degree of obviousness of the violation of law for a reasonable economic entity, together with the availability of sufficient details for the implementation of mechanisms for the protection of rights (Chianale, 1990).

E. CONCLUSIONS

Digitalization or digital economy is an economic activity, the basis of the functioning and development of digital technologies. The innovation of digitalization is increasingly penetrating the daily life of people. It speeds up the exchange of information and increases labour productivity. Information security is the main tool for controlling risks in the digital economy. In conclusion, the creation and operation of an information risk reduction approach will be beneficial if the developed standards are correctly used, if employees are familiar with them, understand their importance and know how to apply them. Therefore, the work must be thoughtful and comprehensive to maintain the company's efficiency.

The sources of financial risks for consumers of digital services can be divided into "human", infrastructural, software, technical, social, and economic. The "human" factor is the most differentiated and least controllable. Consumers of different ages, educational, and professional segments vary in the level of skills in working with digital services, which carries a potential threat of user errors, on the one hand, and makes it possible for services to impose (covertly connect) services without notifying the consumer. Such services may include subscriptions, notifications, etc.

Infrastructure factors are due to the uneven development of the network infrastructure and Internet access, network failures, and a decrease in the transmission and reception speed of the signal. Considering the differences in the infrastructure of dial-up, mobile, channel, and satellite access to the Internet, it is possible to assess the vulnerability of each in terms of the likelihood of losses for consumers. The existence of software factors is caused by vulnerabilities in the software, which become the target of hacker attacks, as well as the obsolescence of anti-virus protection with the active development of a new generation of viruses, including for mobile devices. Economic factors are manifested in the user's costs for access to services, which include the direct purchase of a machine and software, payment for Internet connection and traffic, and additional commissions provided for by several services. Even though contactless payment technologies appeared only in the mid-2000s, and the Apple Pay and Samsung Pay contactless payment systems officially launched in Russia in 2016, they quickly gained customer loyalty, primarily due to their convenience and ease of use. The primary attention in this area should be paid to ensuring the security of applications, the availability of phones with contactless payment technology, and bank terminals with a contactless payment function in large cities and remote areas of Russia.

Direct investment is the most common but challenging way, as it involves allocating budget funds on a competitive basis with a certain amount of lobbying interests and excessive bureaucracy. Direct investments are in some way already morally outdated and no longer have the same effect as before. And nevertheless, direct investment still has significant annual growth in several countries. Tax incentives stimulate enterprises' activities by reducing tax rates for various groups of entrepreneurs. Thus, the state partially loses the inflow of finances received from taxes in the short term, but in the long time, it has a chance to receive an increase in production volumes in the country from each enterprise and the importance of tax collections.

In conclusion, we can say that the potential of tax incentives is tremendous and can fully replace the direct investment system, simultaneously eradicating the problem of lobbying interests. Now, this issue is being actively considered in the legislative assembly, and perhaps in 5 years, the tax system in the country will change dramatically, which will entail an increase in the country's economic potential.

REFERENCES:

Andrianov, V.V., Zefirov, S.L., Golovanov, V.B., Golduev, N.A. (2011). *Ensuring business information security.* Moscow: TsIPSiR: Alpina Publisher.

Aron, R. (1994). *Democracy and totalitarianism.* Moscow: Tekst: Lit.-izd. Study "RIF".

Barber, B. (1984). *Strong democracy: Participatory politics for a new age*. Berkeley and Los Angeles, CA: University of California Press.

Beliaeva, O.A., Vaipan, V.A., Kichik, K.V. (2017). *Public procurement in foreign countries: Dynamics of legal regulation: Monograph.* Moscow: Justicinform.

Bell, D. (1999). *The coming of post-industrial society: A venture in social forecasting.* New York, NY: Basic Books.

Brzezinski, Zb. (1970). *Between two ages: America's role in the technetronic era.* New York, NY: The Viking Press, Inc.

Castells, M. (1996). *The information age: Economy, society and culture,* Vol. 3 End of Millennium. Oxford, UK: Blackwell, 1996.

Chianale, A. (1990). *Obbligazione di dare e trasferimento della proprieta.* Milano, Italy: Giuffrè.

Drucker, P. (1993). *Post–capitalist society.* New York, NY: Harper-Collins Publishers.

Fischer, F. (1991). *American think tanks: Policy elites and politicization of expertise*, In: An international of policy and administrating, pp. 332–353. New York.

Galakhova, A.E. (2011). *Methods of proving of violation of author's rights in informational sphere of Internet.* Rossiiskii Sledovatel, 23, 6-9.

Galbraith, J.K. (1967). *The new industrial state.* Boston, MA: Houghton Mifflin.

Grudtsina, L.Y., Ivanova, S.A., Korotkova, M.V., Shevchenko, L.I. (2018). *The information in civil society.* International Journal of Civil Engineering and Technology, 9(8), 1652-1663.

Grudtsina, L.Yu., Galushkin, A.A. (2013). *Questions of Modern civil society development in the Russian Federation.* World Applied Sciences Journal, 25(5), 790-793.

Habermas, J. (1979). *Communication and the evolution of society.* Boston, MA: Beacon Press.

Izmailov, I.V., Poizner, B.N. (2012). *The complexity of social interactions and Dyakonov-Vinge singularity.* Vestnik Tomskogo Gosudarstvennogo Universiteta, 1(4(20)), 27-28.

Marcuse, H. (2003). *One-dimensional man.* Moscow: AST.

Rostow, W.W. (1960). *The stages of economic: A non-communist manifesto.* Cambridge, UK: Cambridge University Press.

Ryan, A. (2008). *Property,* In: Eatwell, J., Milgate, M., Newman, P. (Eds.), The invisible hand, pp. 312-318. Moscow: Publishing House of the State University Higher School of Economics.

Schelsky, M. (1957). *Die sozialen folgen der automatisierung.* Dusseldorf: Eugen Diederichs.

Shevchenko, L.I., Ivanova, S.A., Grudtsina, L.Y. (2019). *The legal nature of the reinsurance contract.* International Journal of Civil Engineering and Technology, 10(2), 1603-1611.

Singer, P. (1993). *Practical ethics.* New York, NY: Cambridge University Press.

Taranukha, A. (February 20, 2020). *Successful path to digital independence.* Delovoy Peterburg. https://www.dp.rU/a/2020/02/20/Uspeshnij_put_k_cifrovoj

Toffler, A. (1990). *Power shift: Knowledge, wealth and violence at the edge of the 21st century"*, New York, NY: Bantam Books.

Tropynina, N.E. (2020). *Problems and prospects of development of remote banking services in Russia.* Innovatsionnaia ekonomika: perspektivy razvitiia i sovershenstvovaniia, 1(46), 156-161.

Tropynina, N.E., Nikitina, L.N. (2019). *Remote banking: Analysis and development Prospects, In Financial literacy, is the key to the well-being of the population.* Materials of the All-Russian Scientific and practical conference. Saint-Petersburg State University of Industrial Technologies and Design.

Yefimova, L.G. (2017). *Legal aspects of electronic banking transactions.* Courier of Kutafin Moscow State Law University (MSAL), 1, 22-41.