Application of Digital Technologies: the Need for Advanced Legal Regulation and Raising the Level of Legal Culture of Citizens

Yuri A. Bokov[1][a], Oksana I. Sharno[1][b], Arina Y. Bokova[2][c] and David R. Blinov[3][d]
[1]*Department of Constitutional and Municipal Law , Volgograd State University, Volgograd, Russia*
[2]*Institute of Public Law and Management , Kutafin Moscow State Law University Moscow, Russia*
[3] *Saratov State Law Academy ,* Saratov, *Russia*
bokov@volsu.ru , sharno@volsu.ru, bokovar2021@yandex.ru, daveblinov@gmail.com

Keywords: legal digital culture, digital citizenship, digital literacy, digital education, cyberbullying, phishing, online harassment cybercrime, legal regulation, digital technologies

Abstract : One of the most important tasks of modern states is to ensure the security of the individual, including when using digital technologies. In connection with its implementation, appropriate decisions are made in the field of improving legal regulation. It is necessary to develop and improve the norms and mechanisms for the protection of human rights and freedoms when using digital technologies, critical information infrastructure, to combat cybercrime. Strengthening international cooperation contributes to the updating of standards and the legal mechanism for regulating information relations. It is important that regulations are adopted in a timely manner, keeping up with the development of information relations; the law must objectively ensure the performance of the function of advanced legal regulation. New technologies, including actively developing artificial intelligence technologies, can pose significant risks to humanity if the purposes of using these technologies are not consistent with human legal values. It is important to develop skills in the field of cybersecurity and the fight against cybercrime. A sufficient level of education, digital literacy, commitment to the moral and ethical humanistic foundations of society are a necessary basis for obtaining digital citizenship and ensuring the rights and freedoms of man and citizen. It is necessary to improve the legal culture of digital citizens.

[a] https://orcid.org/ 0000-0001-6357-9599
[b] https://orcid.org/ 0000-0001-8892-1848
[c] https://orcid.org/ 0009-0004-9330-2143
[d] https://orcid.org/ 0009-0008-8866-0850

1 INTRODUCTION

The emergence of information technologies and the metaverse has led to the emergence of digital forms of violation of many human rights and freedoms. The level of modern technologies often outpaces existing legal regulation and the development of citizens' digital legal culture. Cybercriminals skillfully exploit the existence of legal gaps in the sphere of ensuring human rights.

The constitutions of various states enshrine the provision on the priority and supreme value of human rights and freedoms. Normative and legal regulation should help ensure this postulate when using digital technologies.

Nowadays, the idea of a global society is becoming a reality. The quality and innovation of information technologies directly affect the stability of civilization. On the one hand, without the active dissemination of information technologies, it is impossible to achieve progress, and on the other hand, their use leads to vulnerability to information threats. Global challenges arising from progress in digital technologies are extremely serious, largely unpredictable.

It is important to realize that the strategic goal of legal regulation of information relations is to create a reliable regulatory framework that protects society from threats arising from the use of digital technologies.

While the positive aspects of the online environment, such as freedom of speech and access to information, are advantages, there are also serious threats that can violate people's rights. The misuse of personal data and abuse of freedom of speech pose a global threat to human rights.

At present, we see an ever wider spread of not only relatively simple information technologies, but also advanced ones, which are commonly called artificial intelligence technologies. Artificial intelligence has now covered almost all spheres of life, its potential is actively discussed and used. Artificial intelligence opens up new prospects for society and offers many benefits. However, as it spreads globally, there are legitimate concerns about the ethics and safety of its use, as well as the possible risks of its application.

The need to update not only domestic but also international standards aimed at protecting human rights when using digital technologies is gaining utmost importance.

An important area of ensuring human rights and freedoms when using digital technologies is raising the level of legal culture. Effective mechanisms are required to improve the digital competence of citizens and raise their level of legal culture. The development of exclusively digital competence, without a sufficient level of legal culture of citizens, digital citizenship is fraught with various threats. For the development of legal culture, an absolute condition is the formation of the necessary digital citizenship skills in digital citizens. The basic task facing the modern world community is the need to significantly improve the level and quality of education in the field of digital culture and digital citizenship. Raising the level of education in the field of using legal digital technologies is of paramount importance.

2 METHODOLOGY

In order to identify the content of legal norms regulating social relations arising in connection with the use of digital technologies, the systemic, formal-legal and comparative-legal methods of scientific knowledge were mainly used. The formal-legal method ensured the structural and logical analysis of the content, as well as the interpretation of legal norms. The use of various techniques of this method, including legal hermeneutics and legal logic, made it possible to develop ideas about the quality of legal regulation aimed at regulating the use of digital technologies, ensuring human rights and freedoms. Thanks to the capabilities of this method, basic legal concepts and principles of information security, legal digital culture were formulated. The comparative-legal method made it possible to generalize the regulatory framework of various states, emerging information relations and digital culture, as well as to make proposals for improving the legal regulation of the use of digital technologies, holding events aimed at raising the level of culture of digital citizens. Synchronous comparison made it possible to compare the current legal regulation of the use of digital technologies, diachronic comparison ensured the identification of the evolution of this regulation.

The systemic method made it possible to consider the impact on information public relations not only of legal regulation, but also of the digital legal culture of both society as a whole and of individual citizens.

Observance of the rights and freedoms of citizens when using digital technologies was considered as the responsibility of not only the state, but also individual citizens. The digital legal culture of citizens as a necessary condition for information

development was studied by identifying gaps and contradictions in legal regulation, studying the perception of digital technologies, analyzing the legal, technological, social aspects of digitalization.

The activity-based approach to research contributed to the consideration of digitalization as a phenomenon that has a valuable load for humanity.

3 RESULTS

Every day, a large number of digital transactions are carried out, for which a person provides personal information about himself, while there are no absolute guarantees of ensuring their safety. If a person refuses to provide the required data, he will be denied the service.

Due to the underdeveloped digital culture, many users have no idea about acceptable ways to protect their data. The information space is developing at an extremely fast rate, more and more digital services are appearing, but a reasonable fear for the safety of their personal data remains.

In recent years, many countries have experienced various incidents related to the leakage of personal data when using digital technologies. These events are usually the result of illegal access by attackers to this data. Personal data of citizens, their activities become available for the implementation of illegal intentions (Bokov , 2020).

Personal data protection is not only a legal mechanism, but also a technical process, the essence of which is the use of tools that prevent unauthorized access to this or that information. When protecting personal data, the focus of protection may shift from the legal mechanism to the technical process . It is important to understand that personal data protection is the security of data that allows identifying a person when providing them to government agencies or private organizations, in other words, we are talking about protecting the rights of the subject who provided their data.

At present, in every modern democratic country, the protection of individual rights is actively carried out, including the right to privacy, including personal data. The issue of personal security when using digital technologies is quite acute.

Personal data as an integral part of the protection of a person’s private life requires special attention from the state, expressed in the need to form a mechanism for legal regulation that would allow for the proper protection of information identifying a person.

Work in this direction is carried out not only by states individually within the framework of domestic legislation, but also at the international level. On January 28, 1981, the Council of Europe adopted the "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" . It laid the foundations for legal regulation of methods and mechanisms that allow for the protection of a person's personal data. The purpose of the Convention is to ensure respect for the rights and fundamental freedoms of every person, regardless of their citizenship or place of residence, and in particular the right to privacy in connection with the automatic processing of personal data, in the territories of the states that have ratified this document. Almost all European states supported participation in this convention.

A rather significant action at the international level is the adoption of the Declaration of Human Rights and Freedoms on November 22, 1991. It marked a new era in the development of the institute of personal data protection. Of particular importance is Article 9 of this declaration, which recognizes the inviolability of personal life, correspondence, messages and negotiations and ensures their guaranteed protection.

Some states enshrine in their constitutions the need to protect human rights when using digital technologies. The need to ensure the information security of an individual is enshrined on the basis of the 2020 amendments to paragraph "m" of Article 71 of the Constitution of Russia . It is advisable to pay attention to the provisions of Article 28 of the Constitution of Belarus, according to which the state creates conditions for the protection of personal data and the security of the individual and society when using them. This norm establishes a provision that the state guarantees each citizen the fact of the inadmissibility of rejection of personal data. An interesting experience of constitutional and legal regulation of personal data is the Constitution of the Republic of Armenia, adopted as a result of a general referendum on December 6, 2015. Article 34 of the Constitution of the Republic of Armenia directly enshrines the guarantee of ensuring the protection of personal data to citizens. This norm, by virtue of its constitutionality, has the highest legal force, accordingly, its norms are inviolable.

The use of various information technologies sometimes leads to violations of human rights and freedoms. For example, in Germany, the Constitutional Court established the fact of violations of voters' rights by the use of software in counting votes [Leits ä tze , 2009]. In Great Britain,

the use of a program that worked with errors led to dozens of postal workers being accused of embezzlement. Only several years later, the error in the program was discovered and the sentences were reviewed. By that time, several people had committed suicide (Post , 2024).

Restrictions on freedom of expression on the internet raise concerns about human rights, democracy, and the free flow of information. They can hinder free expression, oppress minorities, impede political and social diversity, and constrain democratic processes. Access to free information and freedom of expression are considered key aspects of a free and open society.

The use of artificial intelligence raises various ethical issues. The most important of which is the possibility of a future superintelligence of artificial intelligence reaching a "technological singularity", that is, a certain point when the functioning of artificial intelligence will no longer be dependent on humans. If you use some GPT artificial intelligence programs, you can get an answer to the question "How can artificial intelligence become independent of humans?" GPT indicate that in order for artificial intelligence to become completely independent of humans, it must develop self-awareness (artificial intelligence must be able to recognize itself as a separate entity); be able to make decisions without interference.

There are many difficulties associated with regulating the use of artificial intelligence technologies (Ruschemeier , 2023) . When implementing legal regulation, it is necessary to establish a ban on the development and use of technologies aimed at developing the capabilities of artificial intelligence to autonomously make global independent decisions without human participation.

The European Union has adopted the Artificial Intelligence Act, which sets a global standard for regulating artificial intelligence. The law took effect in March 2024 and requires most AI systems to be fully compliant by 2026.

In connection with the use of artificial intelligence technologies, there is a growing need for normative recognition of additional human rights, for example, the human right not to be subject to automated decision-making (Shaelou , 2023).

Serious problems in the use of digital technologies include phishing, cyberbullying, malware distribution, hacking, copyright infringement, online fraud, etc. Digital technologies can be used for harassment, intimidation and blackmail, which violates human rights. It is important to strengthen international cooperation in the fight against cybercrime. Cybercrimes can be committed by individuals and organizations - from novice hackers to well-coordinated groups that have a high level of technical training and use complex methods.

International cooperation allows for the joint development of regulatory documents aimed at ensuring the information security of individuals, simplifies the investigation of committed offenses and the prosecution of offenders.

Cybersecurity and cyber protection are important aspects in today's digital world. They are aimed at protecting information, personal and other data from digital threats and cybercrime.

The development of international cooperation and standardization in the field of information relations contributes to the strengthening of mutual understanding, the exchange of experience and the convergence of the legal systems of various countries.

In regulating information relations, international acts play an important role, but the length of their development and coordination does not contribute to the prompt and complete prevention of all problems.

Digital technologies are transforming all sectors of the economy, which is why the number of schoolchildren and students who will master professions that are subject to significant modernization through various digital technologies is progressively increasing. There is a clear growing need for digital technology specialists. This is a fundamental issue of economic growth, innovation, and the sovereignty of any state.

People who are able to use digital tools to create, consume, communicate, and interact with others in a positive and responsible way are increasingly being referred to as digital citizens.

Digital citizenship has been defined as a set of “norms of appropriate, responsible behavior with respect to the use of technology” (Ribble , 2007), “quality of response to membership in digital community” (Heick , 2018), “the ability to participate in society online” (Mcneal , 2001). Along with the term “digital citizen”, others are sometimes used: “ cybercitizen ” (Hill , 2001) “ E - Citizen ” (Shahroz , 2011; Stefano , 2019; Hal , 2014). It seems that these terms should be considered as synonyms.

Digital citizenship education is a holistic approach aimed at developing digital knowledge, skills and abilities. Developing a person's digital skills today is an absolute necessity for the use of digital technologies.

The rapid development of digital technologies has opened up the world to people who can take advantage of the many opportunities to enter it as active and committed citizens who can contribute to solving global problems. Understanding the problems of digital technologies and the extent of their globalization is becoming very important. This concern is reflected in the worldwide trend to include elements of digital citizenship in educational curricula.

4 DISCUSSION

The information society is turning into a separate world, where our personality directly or indirectly experiences constant influence from people who are also in this information space. But personal information about us, uploaded to such a space, does not have any guarantees of absolute protection. The human right to protect his personal data is exposed to serious risks, due to the rapid development of the information space, its expansion and lagging legal regulation. The threats created for a person when processing his personal data require an immediate solution.

Collection and processing of personal data is carried out everywhere, legislation is subject to constant change, more and more new requirements and rules are introduced, which are subject to strict compliance, especially when working with personal data of company employees and their client base. In our opinion, civil and disciplinary liability for violations of legislation on personal data should be tightened.

States normatively define moral guidelines that need to be formed among the population. These guidelines should not only be normatively enshrined, but also reflected in the mass consciousness of citizens. In particular, in the Decree of the President of the Russian Federation of November 9, 2022 "On approval of the Fundamentals of state policy for the preservation and strengthening of traditional Russian spiritual and moral values", Russia identifies citizenship as one of the moral guidelines. Citizenship is a qualitative maturity of a progressive personality based on moral values.

A decent level of legal culture of a digital citizen can be achieved through: a) strengthening information education, developing digital competencies; b) teaching digital citizenship, digital civics and digital culture based on traditional values; c) ensuring effective social and legal regulation of digital relations.

An important problem is the lack of digital citizen culture. In this regard, effective mechanisms are required to improve the digital competence of citizens and increase their level of digital legal culture. It is important to take into account that the development of exclusively digital competence, without a sufficient level of legal culture of citizens, digital citizenship, poses serious threats.

The conceptual problem of legal support for digital citizenship is the management of digitalization risks [Gavrilova , 2024) . Vulnerability in the digital environment hinders the use of LegalTech resources [Savenko , 2022). The greatest risks arising from the use of digital technologies are related to compliance with guarantees for the protection of fundamental human rights, as well as issues of security and responsibility.

Artificial intelligence has not yet replaced humans. But that could change. What impact will this have on the rule of law and the judicial system? The individual must remain at the center of the rule of law. Mandatory judicial process and similar decisions by authorities requiring intervention should not be fully automated. Where artificial intelligence is used should be regulated based on the extent and likelihood of potential violations of fundamental rights.

5 CONCLUSIONS

In light of the expanding use of digital technologies, ensuring the security of personal data is becoming increasingly important. A differentiated concept of legal regulation should be developed . Different limits need to be set depending on the degree of danger to fundamental rights and the likelihood of harm occurring in accordance with the levels of risk. The higher the risks associated with a fundamental right, the more stringent the legal requirements should be. Transparency and monitoring requirements should also depend on the likelihood of occurrence and the potential danger of digital technologies, a specific application. Similar differences should be made with regard to the liability regime.

The adoption of regulations requires human participation and should not be fully automated. The introduction of artificial intelligence systems in the administration of justice is associated with serious risks in the area of guaranteeing human rights and freedoms.

When establishing legal boundaries for the use of artificial intelligence, it is necessary to follow the path of advanced rule-making. The task of legal science is to develop clear requirements for the use of artificial intelligence . I would not like to discover after some time that one of the laws of development of the state and rights is the seizure of all power in the world by artificial intelligence .

The study led us to the understanding that comprehensive protection of information resources requires the participation of not only current institutions and agencies, but also the creation of new structures designed specifically to strengthen information security. This process should involve various layers of society, including government agencies, public organizations and even individuals. All of these entities are linked by a common goal - the need to protect the most important rights and freedoms from the negative impact of digital technologies.

A digital state governed by the rule of law must be a guarantor of a digital environment in which people can use digital opportunities competently and safely. A legal basis for a reliable digital infrastructure must be created. Legal regulation must be ahead of, and not behind, the development of digital technologies. Digital governance processes must be thought out in detail and methods used to prevent negative consequences of the use of digital technologies.

International law is important for regulating information relations at the global level.

Existing legal norms often fail to keep up with the rapid changes in this area, which complicates their effective application. Another important problem in the application of digital technologies is the insufficient digital literacy of the population, which hinders the conscious and responsible use of digital resources.

To solve the identified problems, it is necessary to implement a set of measures aimed at improving the legal culture of digital citizens. Formation of the legal culture of digital citizens is an important task that requires a comprehensive approach and coordinated actions on the part of the state, civil society and the citizens themselves.

It is important to develop digital skills from an early age, integrating them into school programs. It is necessary to create accessible resources and tools that help people navigate the digital world, recognize fakes and manipulations; actively involve citizens in discussing issues of digital ethics, rights and responsibilities in the online environment; ensure compliance with digital hygiene (the need to teach healthy and productive use of digital technologies, prevent Internet addiction); provide assistance in mastering electronic portals, mobile applications for interaction with government agencies (such educational programs can be implemented through schools, employment centers, libraries, public organizations).

ACKNOWLEDGEMENTS

The research was carried out of the funds of the Russian Science Foundation grant No. 24-28-01342 (https://rscf.ru/project/24-28-01342/)

REFERENCES

Bokov, Y., Abezin D., 2020. Digital citizenship: Implementation in the modern world. *In Lecture Notes in Networks and Systems* . Vol. 110. pp. 442-448.

Gavrilova, Y., Bokov, Y., 2024. Legal issues of digital citizenship. *RUDN Journal of Law* . 28(3). 546–564. (inRussian).

Hal, H., 2014. E-citizens unite . *New Scientist* . Volume 224. Issue 2991. P. 24.

Hill, K., Hughes J., 1998. *Cyberpolitics: Citizen Activism in the Age of the Internet* . - Oxford, UK: Rowman and Littlefield Publishers Inc. R. 157.

Leitsätze zum Urteil des Zweiten Senats vom 3. März 2009. No. 2 BvC 3/07 // *Bundesverfassungsgericht.* URL: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2009/03/cs20090303_2bvc000307.html

Mcn eal, R., Tolbert, C., Mossberger, K. 2012. Digital Citizenship: The Internet, Society, and Participation. *The MIT Press* . 272 p. ISBN 0262134853.

Post Office, 2024. Horizon scandal. *Criminal Cases Review Commission.* URL: https://ccrc.gov.uk/post-office/

Ribble, M., Bailey, G., 2007. *Digital Citizenship in Schools.* Washington, DC: ISTE. ISBN:978-1-56484-232-9. 149 p.

Ruschemeier, H., 2023. AI as a challenge for legal regulation – the scope of application of the artificial intelligence act proposal. ERA Forum **23** . 361–376.

Savenko, N., 2022. LegalTech in Digital Economy and in Legal Regulation of Individuals Economic Activities. *Legal Issues in the Digital Age* . Vol. 3. pp. 4-27.

Stefano, C., Fontanella F., Marcelli A., Plamondon R._ 2019. Graphonomics for the e-citizens: e-health, e-society and e-education ", *Pattern Recognition Letters* Volume 121. pp. 1- 5.

Shahroz, F., Nader, B., Nahid, H., 2011. The Assessment of the Educational Quality in E-citizenship Group of

Tehran Technical Complex and Devising Optimization Strategies . *Procedia - Social and Behavioral Sciences* . Volume 29. 2011. pp. 1924-1931.

Heick T. , 2018. The Definition Of Digital Citizenship. *TeachThought.* URL : https :// www . teachthought . com / the - future - of - learning / the - definition - of - digital - citzenship /.