Legal support of information security of the individual in the conditions of digital transformation of society

Anna Kozyreva[1*], *Galina* Rustikova[2], *Tatiana* Pirozhkova[3], *Valentin* Shelmenkov[4] and *Alexey* Belyavskiy[5]

[1] HSE University, Myasnitskaya str., 20, Moscow, 101000, Russia
[2] The All-Russian State University of Justice (RLA of the Ministry of Justice of Russia) Azovskaya str., 2 bldg. 1 Moscow, 117638, Russia
[3] The Institute of Legislation and Comparative Law under the Russian Federation Government, B. Kharitonievsky Lane, bldg. 22-24/1A, 1BV, Moscow, 107078, Russia
[4] Kutafin Moscow State Law University, 9, Sadovaya-Kudrinskaya str., Moscow, 125993, Russia
[5] Lomonosov Moscow State University, GSP-1, Leninskie Gory, Moscow, 119991, Russia

Abstract. The article considers a comprehensive legal approach to ensuring the information security of the individual in the context of the digital transformation of public relations affecting the spheres of education, obtaining public services, including in the administration of justice, as well as the digitalization of the legal profession. The process of creating the Concept of ensuring the rights and freedoms of man and citizen in the digital space of the Russian Federation, as well as the need for the objective use of personal data in the identification of a person in the information and communication environment, is investigated. An actual international problem is to ensure the information security of the individual in the implementation of rights and freedoms that allow using information and communication technologies to communicate, to obtain relevant and reliable information that affects almost all aspects of life. The experience of various countries, such as China, England, France, in determining approaches to the legal support of information security of the individual, is considered.

1 Introduction

Information security of the Russian Federation is expressed by the legislator as "the state of protection of the individual, society and the state from internal and external information threats. These are the implementation of the constitutional rights and freedoms of man and citizen, decent quality and standard of living of citizens, sovereignty, territorial integrity and sustainable socio-economic development of the Russian Federation, defense and security of the state are ensured.

Information security of the individual (or "state of personal security") at the same time, while not yet defined by law (if we do not take into account the concept of information security of children), nevertheless, rightly arouses the active interest of many scientists, jurists. A number of views were expressed on the definition of the term. Nuyanzinyh [1] proposes in the content of information security of the individual to distinguish several types:

1) information and technical;
2) information and ideological;
3) information and psychological;
4) information and legal.

With the active development of globalization processes [2] and the spread of information and communication technologies in recent years, the spheres of higher education, advocacy and justice have undergone significant changes. Mobile devices and technologies became more accessible, which allowed more citizens to use online products and services. According to international studies, in the first quarter of 2020, there were more than 5.19 billion mobile phone users in the world using the phone as a means of communication, but also as a means to receive various services.

In one calendar year, the increase was 124 million people (2.4%) [3]. The relatively high involvement of the population in the information and communication environment (on average, Russian citizens spend 7 hours and 17 minutes on the Internet, for comparison - in Japan 4 hours and 22 minutes) raises questions of readiness of the state.

It also concerns the existing social and industrial institutions to ensure equality of opportunity and availability of electronic services in the field of education, advocacy, justice, as well as to ensure the protection of personal information and information security of personal personalities. It is not a sign. Topical issues of normative and legal regulation of information security of the individual in the context of globalization are reflected in the works of Russian scientists Chebotareva A.A. [4], Morozov A.V. [5], Polyakova T.A. [6] and others.

* Corresponding author: an.ksandrovna@yandex.ru

2 Materials and methods

The methodological basis of this study has traditionally become general scientific methods: synthesis, analysis, induction and deduction. The method of factor analysis was used to determine the influence of various factors on the information security of the individual.

The information basis of the study was made up of normative legal acts, documents of public authorities and their officials, scientific works of Russian and foreign scientists on information security problems, information and analytical materials of the international level.

3 Results and discussion

One of the novelties in the issue of information security of the individual is the protection of information in the field of attorney-client privilege, which is an important guarantee of preserving the independence of the institute of the bar and maintaining authority and trust in specialists in this profession. At this stage, the Federal Chamber of Lawyers of the Russian Federation is considering a project to create an Integrated Information System of the Bar of Russia (hereinafter referred to as the CIS AR), which should become part of the ecosystem of the digital economy of the Russian Federation as a whole through integration with existing state information systems.

In particular, it is planned to create a personal account of each lawyer within the framework of the CIS AR as an electronic digital space as a way to organize advocacy.

It should be noted that this innovation in the creation of an electronic personal account of a lawyer, the possibility of active use of an electronic lawyer's request, as well as attempts by law enforcement agencies and supervisory authorities to obtain information from a lawyer that is a lawyer's secret require uniform legislative regulation.

It also requires the creation of increased guarantees for the protection of information constituting attorney-client privilege, including in order to ensure information. Personal security. At the moment, the greatest attention is drawn to the requirement that the lawyer have a qualified electronic signature.

At the same time, it should be noted that the use of modern information technologies in judicial activities has already become a global trend. Currently, in England, it is possible to not only file petitions for a lawsuit and perform public duty via the Internet, but also to monitor the progress of the case. Both parties to the process fill out standard electronic forms without visiting the court in person. Moreover, this possibility, unlike a direct visit to the court and the transfer of documents in person, is not limited by time frames: you can deliver documents electronically around the clock and on any day. French civil procedure allows for electronic documents and/or proceedings by electronic means.

With regard to the digitalization of justice in the Russian Federation, it should be noted that in the system of courts of general jurisdiction, the Supreme Court of the Russian Federation, the supreme courts of the constituent entities of the republics, regional courts, regional courts, courts of cities of federal significance, courts of the autonomous region, courts of autonomous national districts, national districts (fleets) of military courts, correctional institutions and colonies of the Federal Penitentiary Service of Russia are provided with a video conferencing.

Video conferencing in the system of courts of general jurisdiction is used in various situations, including in criminal proceedings. However, unlike criminal and arbitration proceedings, the procedure for conducting video conferencing is not regulated by civil procedural legislation [7].

In the Doctrine of Information Security [8] in 2016, one of the information threats is indicated by a high "level of dependence of the domestic industry on foreign information technologies." One of the available solutions to the problems of information security, for example, the educational process is the import substitution of software (hereinafter referred to as the software).

Until August 1, 2021, it is planned to implement a pilot project on import substitution of software in the field of science and education, for the implementation of which the Ministry of Statistics of Russia, Bauman MSTU and «Voskhod» Research Institute are responsible. "We are talking about two groups of software: software that provides educational activities and software used in the educational process. These are antiviruses, browsers, help systems, software for working with graphics, office, high-quality engineering software that is used to prepare students", Dmitry Chernyshenko, Deputy Prime Minister of the Government of the Russian Federation, said.

The introduction of digital identification systems around the world is being developed to ensure the privacy of citizens. For example, in the UK, a digital strategy has been developed. This document includes a section "Economics of data" – expanding the possibilities of using data in the UK economy and increasing public confidence in their use [9].

There are many threats and risks associated with whether we all have to identify constantly and end-to-end, or we need to impose some kind of restrictions. How to find a balance between private and public interests? This question is the most relevant among both theorists and practitioners of law. It is assumed that there is a need to introduce a new concept, such as "identity mystery".

A person must be sure that what he does, he does voluntarily, these actions are not imposed on him by anyone (of course, there are exceptions within the law), and all the information that arises as a result of his decisions behind a computer monitor, laptop or smartphone screen is used only for those purposes for which he is identified. Otherwise, personal information may appear in the information and communication environment, access to which should be legally restricted.

eIDAS[a] regulations defines electronic identification as "the process of using a person's identification data in electronic form that uniquely represents a natural or legal person", which regulates the development and use in the EU of electronic identification and trust services (including electronic signatures and seals, time stamps, site authentication and electronic delivery) [9].

Thus, a new mass phenomenon has already appeared – digital identification. Thus, Article 11 of Law No. 152-FZ states that biometric personal data is understood as information characterizing the physiological and biological characteristics of a person that is used by the operator to establish the identity of the data subject.

On December 10, 2020, the President of the Russian Federation, together with the Presidential Council for the Development of Civil Society and Human Rights (hereinafter referred to as the Council) developed a draft concept for ensuring the protection of human and civil rights and freedoms in the digital space of the Russian Federation (hereinafter referred to as the Concept). There was a draft action plan ("road map") for its implementation including measures to improve the digital literacy of citizens of the Russian Federation and their training in information security and digital hygiene skills.

The analysis of incoming appeals to the Council made it possible to identify the main threats to the information security of the individual arising in the information and communication environment. Cyberbullying, manipulating the opinion of citizens on the basis of information and communication devices collected with the help of computers, smartphones includes related information and communication devices for transmitting information (so-called digital traces and digital shadow) [11].

There is the use of facial recognition technologies and the use of gra images obtained as a result, zhdan (in the GIS "Unified Data Storage Center - ECCD through the automated information system "Access Control System to Information Systems and Resources of the City of Moscow" (SUDIR)), digital inequality, digital illiteracy, etc.

The developed concept "will contain such aspects of protecting citizens from digital threats as educational, technological and regulatory - determining how the legislation that regulates the relations arising in the digital sphere should develop further. And there are data whether there is a need to streamline the existing norms of different laws through the adoption of the so-called digital code" [12].

With the introduction of modern digital technologies with a wide declaration by the Constitution of the Russian Federation of human and civil rights and freedoms, the legal insecurity of the individual in the information and communication environment remains obvious. The current situation requires regulatory regulation, including the application of the norms of "soft law".

One of the options for solving the problem may be the development of the above-mentioned Concept, which will reflect the main threats to human rights and freedoms in the context of the development of the information and communication environment and global digitalization, as well as identify possible ways to prevent them.

The first threat is cyberbullying (meaning any electronic communication using technology, including but not limited to computers, other electronic devices, social networks, text messaging, instant messaging, websites and email, usually repetitive or with ongoing effects. That causes fear, intimidation, humiliation, anxiety or other damage or harm to another person's health, emotional well-being, self-esteem or reputation, and includes facilitating or encouraging such communication in any way), the victims of which are not only minors, but also adults.

The Convention on the Rights of the Child states that measures to combat intimidation, including cyberbullying, should be strengthened, which include prevention, early detection mechanisms, and the empowerment of children to use the information and communication environment as a source of information [13].

The second threat is the manipulation of citizens' opinions on the basis of the collected information in the information and communication environment using computers, smartphones, as well as related information and communication devices (and it is important to keep in mind that such information is voluntarily reported by the owners of the devices in the process of their use).

The third threat is the developing practice of installing surveillance cameras on the streets and in urban transport using artificial intelligence technologies for facial recognition, which allows one, in fact, to obtain information about the movement of any individual.

The fourth threat is the elimination of the digital divide. In the UN 2030 Agenda for Sustainable Development, Member States recognized the importance of expanding information technology, communications and global interconnections, stressing the need to address deep digital inequalities and develop societies based on a universal, equitable and non-discriminatory approach [14].

China's experience in determining the information security of the individual is interesting. On the one hand, the protection of personal information has been elevated to the status of a separate civil law in the legal field of China. On the other hand, it is planned to establish individual rules in accordance with the criteria for the nature of information, the degree of information processing and the elements of damage that arise when two rights coincide in judicial practice.

Thus, scholars and practitioners are debating a balance of interests in which it is possible to ensure the protection of personal information and confidentiality, while harmonizing the Law on the Protection of Personal Information in the Future in China [15].

[a] eIDAS -electronic IDentification, Authentication and trust Services. URL: https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation (24/04/2021)

4 Conclusions

The digital divide is manifested not only in the lack of a fundamental opportunity for a number of citizens to use new technologies. But this shown in different levels of digital literacy of the population, and it exacerbates another very serious threat.

Citizens cannot resist telephone or Internet fraud, not only because they do not know how to behave in such a situation, but also because in principle they are not aware of the existence of such fraudulent practices. This is a single trend all over the world.

At the moment, a small number of activities are being carried out to improve information literacy, while not covering all age and social groups of the population. People of retirement age are in a state of low awareness of possible threats in the digital space. In connection with this fact, special attention should be paid to conducting educational activities on computer fraud.

Italian Legislative Decree No. 82/2005, article 8, declares that the State encourages initiatives aimed at disseminating a digital culture among citizens to promote the development of skills and the use of digital services [16]. This approach is at the same time the application of the instrument of "soft law" in the process of state regulation while preserving the rights and freedoms of man and citizen in the information and communication environment.

In connection with the above, the inclusion in various educational programs, sections devoted to the formation of legal literacy and digital media - literacy using the information and communication environment, including the Internet as a "knowledge space", will be an important step towards ensuring an information personality. It is important to note that the skill of critical evaluation of information obtained from various sources can also be included in educational programs of various levels.

In conclusion, we would like to note that at the level of state strategic documents, the legal foundations for the formation of the foundations of information security of the individual have been laid. The time has come to move on to the practical implementation of the tasks assigned to theorists and practitioners of ensuring information security of society in general and the individual in particular.

Definitely, the use of new tools for communication and interaction between society and the state greatly simplifies complex bureaucratic procedures and allows you to quickly receive up-to-date information on almost any request.

At the same time, responsibility for the formation of digital traces and digital shadow, including when using biometrics, as well as the potential for the use of information and psychological impact, indicates that the issues of digital literacy of the population, digital hygiene (cyber hygiene) [17] should be reflected in educational programs of various levels.

Only thanks to an integrated approach both on the part of the state to the legal support of protection and on the part of individuals developing, including in the information and communication environment, aware of the consequences of their actions and having sufficient knowledge about existing potential threats, it is possible to ensure information security of the individual in the context of the digital transformation of society.

References

1. S. Nuyanzin, O. Nuyanzin, Legal science and law enforcement practice, **2(44)** (2018)
2. R. Robertson, *Globalization: Social Theory and Global Culture,* pp. 32-34 (SAGE Publications ltd, 2000)
3. Digital use around the world 2020, Global Report, We are social ltd. Retrieved from: https://wearesocial.com/digital-2020
4. A. Chebotareva, Lawyer, **6** (2010)
5. A. Morozov, Bulletin of the Russian Law Academy, **4,** 90-96 (2017)
6. T. Polyakova, Law Enforcement Monitoring, **2(35)**, 53-58 (2020)
7. *Justice in the Modern World:* monograph, p. 454 (Statut, Moscow, 2013)
8. On approval of the Doctrine of Information Security of the Russian Federation: Decree of the President of the Russian Federation 05.12.2016 No. 646 (2016)
9. UK Digital Strategy, 1 March 2017, Department for Digital, Culture, Media & Sport and The Rt Hon Karen Bradley MP (2021). Retrieved from: https://www.gov.uk/government/publications/uk-digital-strategy
10. Practical Law Media & Telecoms. European Commission consultation on Electronic Identification Regulation (2020)
11. G. Rustikova, Information law, **3(61),** 29-32 (2019)
12. HrC intends to prepare this year a concept for the protection of human rights in the digital environment (2021). Retrieved from: https://www.garant.ru/news/1412161/
13. Convention on the Rights of the Child: Concluding Observations on the Combined Fifth and Sixth Periodic Reports of Belgium, UN H. R. C., 2 WLUK 786 (2019)
14. Int'l Ency., Cyber Law, 2928408 (2020)
15. Shujie Cui, Peng Qi, Computer Law & Security Publisher: E (2021)
16. Decreto legislativo n. 82 - Codice dell'amministrazione digitale. (G.U.16 maggio 2005, n. 112 - S. O. n. 93) (2005)
17. A. Kozyreva, Gaps in Russian legislation, **7,** 92-94 (2018)