International Legal Mechanisms for Ensuring Digital Security

Gafur Mansurov

Ural State University of Economics, 620990 Ekaterinburg, Russia

Abstract. The main purpose of this article is to analyze the system of international legal regulators that ensure digital security. The author draws attention to the complexity of interpreting the content of the concept of "digitalization" and substantiates the impossibility of constructing a generally accepted definition. The paper identifies the features of digitalization risks. The analysis of the main international legal acts ensuring digital security has been carried out.

1 Introduction

Nowadays, humanity witnesses the beginning of a new fourth technological revolution the result of which will be the massive introduction of cyber-physical systems into production. According to the President of the World Economic Forum, Klaus Schwab, of the many diverse and exciting challenges facing modern society, the most important and impressive is the awareness and formation of a new technological revolution. In his opinion, we are at the origins of a revolution that will fundamentally change our life, work and communication. In scale, scope and complexity, this phenomenon, which he calls the fourth industrial revolution, has no analogues in all the previous experience of mankind [12, p.9].

Its most important goal, as you know, is the digitalization of all spheres of public relations. As a result, new technologies become the object of economic turnover. This, in turn, entails the need for legal regulation of the creation, change and termination of relations arising from digital technologies.

It is obvious that the digital revolution will make serious adjustments to the system of measures to ensure economic security in general, and digital security in particular. There will be both new threats and new measures to ensure security, including measures to ensure security against old threats that arose in the pre-digital era.

The problem is aggravated by the fact that the digital revolution coincided with another aggravation of the geopolitical situation, one of the manifestations of which is the so-called digital wars. Some experts express their opinion about the beginning of the "digital cold war between Washington and Moscow" [13]. Moreover, the US sanctions against the Chinese company Huawei qualify as the beginning of the first digital war [4]. Hostile measures are also being taken against the Russian Federation, for example, the shutdown of Gazprom's compressor stations through the orbital system at the request of a foreign manufacturer, the suspension of the operation of machines with an imported numerical program device at factories of the military-industrial complex, etc. [7].

At the same time, from the point of view of the rules of legal technique, i.e. a set of methods, means and techniques used in the development and systematization of legal acts [1, p.482], the use of the term "war" is incorrect primarily due to the extreme vagueness of the content of this concept. Therefore, one should agree with the statement that such “information wars” (“cyber wars”) need to be comprehended and viewed as a separate legal category of conflict relations between states, possibly using *slightly different criteria that are used in traditional approaches to defining the concepts of war and armed conflict* (italics is mine – G.M.) [8, p.14].

Thus, the article aims to analyze the system of international legal regulators that ensure digital security.

2 Materials and Methods

The materials of the study were primarily international treaties and acts of international organizations. In addition, doctrinal studies of domestic and foreign specialists were studied.

When analyzing the material for the study, standard methods of research of legal phenomena were used: formal dogmatic, systematic and logical ones. The formal dogmatic method is of particular importance in the context of the research topic.

3 Results and Discussion

As a result of the analysis of the content of regulations and literature, it was found that there is no uniform interpretation of the concept of "digitalization". This circumstance creates significant difficulties both in the development of draft regulations and in their implementation. Currently, there are already several dozen such definitions of the above category. Moreover, some of them are very curious. So, for example, according to one of the documents, digitalization tasks include, in particular, maintenance of printing press (order of the Ministry for the Development of the Russian Far East “On approval of the Informatization Plan of the Ministry of the Russian Federation for the Development of the Far East for the 2018 financial year and the planning period of 2019 and 2020”). Obviously, the new term “digitalization” should be used to refer only to those results of the technological process that were involved in the economic turnover in connection with the digital revolution. Its most important result, as you know, is the creation of a digital platform.

A digital platform in special literature refers to a system of algorithmic relationships between a significant number of market participants united by a single information environment, leading to a decrease in transaction costs through the use of a digital technology package and changes in the division of labor. Platform solutions are platforms or digital services that are platforms or their elements (Action plan for "Normative regulation" of the program "Digital Economy of the Russian Federation", approved by the Government Commission on the use of information technologies to improve the quality of life and conditions for doing business, protocol of December 18, 2017 No.2). The most important platform is blockchain. That is why the term "digitalization" in this case should be understood as blockchain.

In its most general form, a blockchain is a software product that allows you to store data and conduct transactions over the Internet without intermediaries. For example, in 2017, in his speech at the St. Petersburg International Economic Forum, First Deputy Prime Minister Igor Shuvalov said: “Blockchain is now the number one priority. The President understands that significant growth rates can only be achieved through the introduction of the digital economy and technological leadership” [14].

Nevertheless, the word "digitalization" is now very often used as a synonym for the word informatization, less often instead of the words software and computerization.

Informatization, according to the currently inactive federal law on information, informatization and information protection, means the organizational socio-economic and scientific-technical process of creating optimal conditions for meeting information needs and realizing the rights of citizens, government bodies, local governments, organizations, public associations based on the formation and use of information resources.

In specialized literature it is noted that this term at one time found widespread use only in Russia and China. This was due, firstly, to the insufficient development in the 1980s-1990s of a glossary on the topic “information technologies” and “information society”, and secondly, with some specific features of the development of information and communication technologies in these countries. They were characterized by a high level of development of applied and specialized hardware and software systems and an extremely weak telecommunications infrastructure, which hindered harmonious development of the information society.

According to the doctrinal interpretation, softwarization (from the English ‘software’) means “the development in software of any functions, logic, methods that contribute to the processing of huge amounts of information data” [5, p.111].

As stated in the first Russian dissertation on digital law, the use of the “digital” element in the concept of “digital data” allows us to emphasize that only data that can be processed by a computer are included here [10, p.24]. This opinion is shared by some experts in intellectual property law [2, p.78].

Moving on to analysis of international legal mechanisms for ensuring digital security, it should be noted that among the most important threats is the high level of Russia's dependence in the field of digital technologies, due mainly to the semi-peripheral nature of the domestic economy. However, Russia does not belong to the classic semi-peripheral, let alone peripheral countries. It has a powerful scientific potential, which allows us to hope that the prospects for creating a sovereign segment of the Internet are real. The formal legal basis for such a conclusion is the adoption of a number of special regulations aimed at ensuring the security of the domestic sector of the Internet. The basic act is the so-called Law on the Sovereign Internet. This name was given to the law on amending the laws "On Communications" and "On Information, Information Technologies and Information Protection", which provides for the creation of a national routing system for Internet traffic and centralized management tools.

In addition to Russia's dependence on a number of countries in the field of digital technologies, experts point out the following threats that are of major significance: vulnerability of information infrastructure, cyber terrorism, cyber espionage, interference in the internal affairs of other countries through the abuse of the use of information and communication technologies [6, p.88].

It is fundamentally important that, as indicated in the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030, international legal mechanisms that make it possible to defend the sovereign right of states to regulate the information space, including in the national segment of the Internet, do not exist. In addition, the Strategy notes that most states are forced to constantly adapt state regulation of the information and information technology sector to new circumstances.

Researchers reasonably state that one of the key factors in ensuring long-term international stability in the conditions of the formation and rapid evolution of modern digital society is the formation of a regime of collective responsibility in the sphere of the functioning of the global Internet [3.C.14]. However, economically developed countries are currently pursuing a policy of polarizing international security.

Nevertheless, in order to eliminate or minimize the risks mentioned above, international legal acts of different legal force have been adopted. The most important general international treaties include the Charter of the International Telecommunication Union.

Of the declarative documents, the most important one is the Okinawa Charter of the Global Information Society. This document contains the following rules establishing the need to eliminate the isolation of countries in the field of information and knowledge (digital divide): the principle of promoting competition in the telecommunications sector, protecting intellectual property rights in information technology, developing cross-border electronic commerce in the context of the strict framework of the World Trade Organization, continued the practice of exempting electronic transfers from customs duties until it is reviewed again at the next ministerial conference of the World Trade Organization and the development of a mechanism for protecting consumer privacy, electronic identification, electronic signature, cryptography and other means of ensuring the security and reliability of transactions.

The growing importance of acts adopted within the framework of the Eurasian Economic Union is evident, for example, such is the decision of the Supreme Eurasian Economic Council "On the main directions for the implementation of the digital agenda of the Eurasian Economic Union until 2025".

The most important special acts of the post-Soviet countries are the Convention on Crime in the Field of Computer Information and the Agreement on Cooperation of the CIS Member States in the Fight against Crimes in the Field of Computer Information.

It should be noted, however, that the position of the Russian Federation with respect to the above Convention on Crime in the Field of Computer Information has experienced certain hesitations. The Russian Federation signed this document, but then withdrew it, since the convention contains provisions that can be considered a violation of the sovereign rights of the participating countries. For example, this document provides for the possibility of conducting so-called cyber operations on the territory of a sovereign state without coordination with it. But certain provisions of this document, nevertheless, were subsequently included in the Criminal Code of the Russian Federation in the form of Article 159.6 "Fraud in the field of computer information." According to this rule, theft of someone else's property or the acquisition of the right to someone else's property by entering, deleting, blocking, modifying computer information or otherwise interfering with the functioning of storage, processing or transmission of computer information or information and telecommunication networks is punishable.

In addition, at present there is a serious dilemma between mutually exclusive options for determining the powers of states in the field of ensuring digital security due to the need to take into account the content of international humanitarian law. For example, UN Secretary General Ban Ki-moon, speaking on December 15, 2015 at a meeting of the UN General Assembly dedicated to the review of the implementation of the decisions of the World Summit on the Information Society, called on the fight against cybercrime to prevent violations of human rights and restrictions on freedom of speech [eleven]. This provision is also enshrined in some regional acts, in particular, acts of the Council of Europe, which in one of its documents noted that the effective protection and promotion of democracy, human rights and the rule of law in the digital world are tasks and goals common for many stakeholders (Strategy Council of Europe Committee of Ministers "Internet Governance" - Council of Europe Strategy ").

Nevertheless, the UN General Assembly adopted the resolution “Countering the use of information and communication technologies for criminal purposes” proposed by the Russian Federation by a majority vote, despite the assertions that the content of the document does not comply with the norms of humanitarian law. This resolution establishes the sovereignty of states over their information spaces.

However, the ultimate goal of the Russian side is to secure the sovereign law of the state by an international treaty: “the development, production, accumulation, use, proliferation of information weapons, as well as the use of information weapons methods should be prohibited. The convention on ensuring information security should provide for a mechanism for controlling information weapons, in which the UN Security Council plays a key role [9, p.17].

4 Conclusions

1. The term "digitalization" should be used to refer only to those results of the technological process that were involved in the economic turnover in connection with the digital revolution. However, the content of the concept of "digital security" in international legal acts boils down to ensuring the security of Internet users.
2. Digitalization of public relations has become a powerful stimulus for the development of domestic branches of law. International legal industries have proven to be more conservative.
3. Among the most important threats to our country is the high level of dependence of Russia in the field of digital technologies, due mainly to the semi-peripheral nature of the domestic economy. Significant threats include the vulnerability of information infrastructure, cyber terrorism, cyber espionage, interference in the internal affairs of other countries through the misuse of information and communication technologies.
4. Currently, the process of creating an international legal mechanism for ensuring digital security is underway. The main outlines of architecture are indicated mainly in regional acts. The overwhelming majority of universal acts are advisory in nature.
5. There is currently no universal international legal mechanism. Due to the fact that international relations are entering the next phase of acute confrontation, one cannot expect it to be worked out in the foreseeable future.

References

1. S.S. Alekseev, General theory of law (2008)
2. S.I. Boldyrev, *Copyright for objects posted on the Internet and their protection in the Russian Federation* (2020)
3. S.V. Volodenkov, Bulletin of the Volgograd State University, Series 4: History, Regional studies, **25(3)** (2020)
4. Dmitry Peskov in Kazan: "The First World Digital War has begun today, https://news-life.ru/
5. E.Yu. Zhuravleva, Sociological research, **4**, 109 (2019)
6. L.P. Zveryanskaya, Dynamics of information security institutions. Sat. scientific papers, 84 (2018)
7. E. Kasmi, *Kaspersky asked Putin to quickly transfer banks and government agencies to Russian software*, https://www.cnews.ru/
8. A. Ya. Kapustin, J. of Russian law, **8**, 10 (2015)
9. A.V. Kubyshkin, *International legal problems of ensuring the information security of the state* (2020)
10. K.A. Mefodieva, Digital data as an object of civil law regulation in Germany, the USA and Russia (2019)

11. Pan Ki-moon urged to achieve the elimination of the digital divide and security in the World Wide Web, https://news.un.org/
12. K. Shwab, The fourth industrial revolution (2017)
13. S. F. Cohen, Washington's Dr. Strangeloves Is plunging Russia into darkness really a good idea?, www.thenation.com/
14. Blockchain, www.blockchain.ru/