Forum: Human Rights

Issue: Protecting the right to privacy in the digital age

Student officer*:* Anna Shumeyko

Introduction

The problem of compliance with private law in the period of global digitalization is becoming more serious and necessary to solve every year. The development of information technologies over the past two decades has led to the formation of a new, so-called digital reality. We are talking about creating a new reality that has no analogues in the previous world - the Internet of things, the digital economy, cryptocurrencies, etc.

However, in the legislation of many countries there are still no points that guarantee the protection of human rights in virtual reality. With the advent of digital technologies, so-called digital rights arise. Digital rights are understood as the rights of people to access, use, create and publish digital works, to access and use computers and other electronic devices, as well as communication networks, in particular the Internet. They also include the right to freely communicate and express opinions on the Internet and the right to privacy of the information sphere, including the right to confidentiality, anonymity of his\her already digitized personal information.

Unfortunately, numerous sources of information about literally every person, his sphere of activity, etc. can often be used for the purpose of criminal activity: blackmail, distribution of false information, terrorist acts, robberies by recoding various personal data, distribution of narcotic drugs. For this reason, it is necessary to determine the possible limitations of digital rights by Federal law, including the permissible limits of control of the information environment by law enforcement agencies in order to ensure effective protection of society from cybercrime.

Nonetheless, the creation of such a system of regulation of digital relations also requires detailed study and attention, since they must satisfy both the private right of the individual and the provision of public and state security. A clear example of the imperfection of existing systems is the conflict over the failure of Telegram Messenger to meet the requirements of the FSB of Russia to provide means of decrypting messages. Law enforcement agencies in other countries face similar problems.

All this testifies to the need to search for an optimal legal compromise in the legislative regulation between the possibility of access of law enforcement services to computer information and the right of citizens to its confidentiality.

Definition of key words

Digitalization – widespread adoption of digital technologies in various spheres of life: industry, economy, education, culture, service, etc.

Cryptocurrencies – digital money that exists only in the form of virtual coins and is created in the network without the participation of real money. Cryptocurrency can be stored in special electronic wallets and transferred between wallets directly, bypassing banks. There are more than 2500 types of cryptocurrencies.

Digital rights – human rights, which include the right of people to access, use, create and publish digital works, access and use computers and other electronic devices, as well as communication networks, in particular, the Internet. Internet access is recognized as a right under the laws of a number of countries.

Cybercrime – a set of crimes committed in cyberspace using computer systems or computer networks, as well as other means of accessing cyberspace, within computer systems or networks, and against computer systems, computer networks and computer data.

Background information

The problem of protecting the right to privacy in the digital age has become a global one with the development of digital technologies and virtual reality and it has been around for about 40 years.

Due to the lack of a clear and well-developed system for protecting the rights of citizens in digital reality, the number of cybercrimes related to the use of personal data is increasing every year. Of the public ways of committing cybercrime, we can note 2 types: social engineering and virus programs. Social engineering is described as "the manipulation of a person or group of people to break into security systems and steal important information." The first type consists of a telephone or computer attack on a person in order to obtain personal data. Resorting to the peculiarities of personality psychology, scammers impersonate another person, thereby misleading the person. This psychological method is used by a narrow circle of specialists in the field of information security in order to describe ways to "fish out" personal data, which is based on

knowledge of the characteristics of human psychology, with the use of blackmail and abuse of trust. The most popular method of social engineering is considered to be fraudulent phishing, or "fishing" from illiterate Internet users of their confidential information to access Bank accounts.

Another type of cybercrime that violates personal human rights is considered remote hacking of a computer, through which hackers have the ability to read and edit documents stored on file servers and on computer desktops, have the ability to enter their own malicious programs, and in addition, to collect various kinds of information, information, using audio and video surveillance. The specificity of the second type of cybercrime is that it allows hackers to remotely control computers without the knowledge of their users, using advanced and modern software.

During the entire existence of virtual reality, there have been a huge number of cases of violation of private rights of citizens in different countries, several of which have led to irreversible consequences and disasters.

For example, in January 2018, a group of unknown people in WhatsApp started sending messages to Indian users, which offered to get access to the Aadhaar database for 500 rupees. As a result, the passport data of more than 1.1 billion people in the country became available to anyone. Almost 98% of India's population was under threat.

Another case occurred in the United States. The Facebook company Cambridge Analytica collected data from more than 87 million accounts without the consent of Facebook and users themselves, and also used a vulnerability in the Facebook code to gain access to personal messages. According to the official version of the investigation, the data was used to "profile the electorate" — that is, to identify the political beliefs of American users of the social network. US intelligence agencies claim that this was done deliberately to prepare for the victory of President Donald Trump in the elections in 2016. In September 2018, the investigation data was finally disclosed.

Numerous hacks of personal data became the basis for the creation of various organizations and associations to address the issue of protecting the private rights of citizens in the digital space. One of the largest such organizations is «European Digital Rights» (EDRi) - an international public organization for the protection of human rights on the Internet. The purpose of the organization is to promote, protect and support human rights on the Internet and in the field of infocommunications and technologies. EDRI deals with issues such as personal data protection, digital rights, privacy and anonymity on the Internet, as well as copyright and freedom of speech in the European Internet space. The organization consists of 34 companies from 21 European countries.

Existing measures to develop and promote programs to protect the private rights of citizens in the digital space are not enough. For this reason, a solution to this problem must be found immediately.

Previous attempts to solve the issue

The need to recognize and protect digital rights is proclaimed in a number of international legal acts.

Okinawa Charter on Global Information Society (July 22, 2000)

The Charter was adopted by representatives of eight leading world powers. As fundamental rules, the Charter provides for:

a) development of an effective mechanism for protecting the privacy of the consumer, as well as the protection of privacy in the processing of personal data, while ensuring the free flow of information;
b) further development and effective functioning of electronic identification, electronic signature, cryptography and other means of ensuring security and reliability of operations;
c) the duty of States to coordinate their actions to create a secure cyberspace, security of information systems protected from crime, including transnational organized crime.

UN General Assembly Resolution No. 68/167 of 18 December 2013 "The Right to Privacy in the Digital Age".

The Resolution calls on all States:

a) respect and protect the right to privacy, including in the context of digital communication;
b) put an end to violations of these rights by ensuring that national legislation complies with their international obligations;
c) review its procedures, practices and legislation relating to the tracking, interception and collection of personal data, including mass surveillance, interception and collection, in order to protect the right to privacy by ensuring the full and effective implementation of all international obligations;
d) establish a new or continue to use the existing independent, effective domestic oversight mechanisms.

Possible solutions

1) Strengthening control over cyberspace, immediate response to the emergence of various kinds of "death groups" and other similar communities that call for violence and spread the ideology of the criminal world, as well as strengthening the special control of law enforcement agencies over the shadowy Internet, where the active sale of drugs, weapons and recruitment for terrorist organizations.
2) Creation of a unified cybersystem of state control, when every enterprise that can affect people should be constantly monitored at the Federal and regional level.
3) Development and application of decision algorithms for each type of emergency: cyberterrorism, theft of personal data and secret information.

Useful links

https://en.m.wikipedia.org/wiki/Digital_rights

https://en.m.wikipedia.org/wiki/European_Digital_Rights

https://daccess-ods.un.org/TMP/8867625.5941391.html

https://www.mofa.go.jp/policy/economy/summit/2000/documents/charter.html