ATLANTIS PRESS

Advances in Economics, Business and Management Research, volume 105

1st International Scientific and Practical Conference on Digital Economy (ISCDE 2019)

Legal regulation of counteraction to administrative offenses in the conditions of digitalization

Sultanov K.A.
All-Russian Advanced Training Institute
of the Russian Federation Ministry of the Interior,
Domodedovo, Russia
mpkr@mail.ru

Kashkina Ye.V.
All-Russian Advanced Training Institute
of the Russian Federation Ministry of the Interior,
Domodedovo, Russia
000049@bk.ru

Ustinov P.V.
All-Russian Advanced Training Institute
of the Russian Federation Ministry of the Interior,
Domodedovo, Russia
mvd.kafedra7@yandex.ru

***Abstract* — The paper discusses the legal aspects of the security of the information society through the prism of criminal law and administrative science, identifies the most important issues, and suggests ways to solve them. The analysis of crime acts and offenses in the digital environment, committed with the use of digital technology, as well as proposals to improve measures to combat crime in the field of digital technology are being carried out. The manuscript analyzes the trends in the development of legal regulation under the condition of the digital revolution, digital technology, the new realities of "digitalization" of social institutions, including the institution of law. The authors come to the conclusion that there is a need for a new look at legal institutions in the era of the information society and digital technologies, the consistent adaptation of traditional legal mechanisms to new conditions. Undoubtedly, the control and supervision of the digital environment in the Russian Federation needs to be strengthened and improved in order to ensure information security. In this regard, the issue under consideration actually has high relevance and legal significance. The authors attempted a peculiar interpretation of the modern electronic (digital) environment, taking into account the existing regulatory legal acts in the Russian Federation and foreign legislation. Extraordinary proposals, which will be useful for all categories (levels) of readers with the aim of resolving some controversial issues of protecting the rights of citizens in the digital environment, have been put forward.**

Keywords* — *digital economy, digital environment, digital rights, industrial Internet, digital imperative, digitalization, offense.

I. INTRODUCTION

Currently, any citizen in the world cannot imagine himself without a mobile phone or laptop with access to the Internet. In a close past, in the 90s of the twentieth century, people could not even think that, being, for example, in Germany, they could submit an application on providing a public service in Moscow, Russian Federation, through a digital portal. The rapid growth of digitalization in almost all spheres of life has outlined the paramount tasks for lawyers around the world, i.e., the legal regulation in the digital environment. Lawyers need the formation of a new regulatory environment that provides a favorable legal regime for the emergence and development of modern technologies, as well as for the implementation of economic activities related to the use of digital technologies [1]. Cases of limiting the scope of the digital environment are very rare, while society reacts very negatively to this. Public demand for the consumption of services in the digital environment is growing every day. Recently, in connection with the development of technology, the role of electronic document management has increased. Gradually and steadily, new digital technologies penetrate into all spheres of our life significantly affecting the development of social relations. Digitalization, as the main nowadays trend, prompts us to seriously adjust the activities of established state institutions.

According to a study of 2016, the Russian Federation ranks 41st in terms of readiness for the digital economy, with a significant lag behind the leading countries, such as Singapore, Finland, Sweden, Norway, the USA, the Netherlands, Switzerland, the United Kingdom, Luxembourg, and Japan. In terms of the economic and innovative results of using digital technologies, the Russian Federation ranks 38th with a huge lag behind the leading countries, such as Finland, Switzerland, Sweden, Israel, Singapore, the Netherlands, the USA, Norway, Luxembourg, and Germany [2].

Such a significant lag in the development of the digital economy behind the world leaders is explained by gaps in the regulatory framework for the digital economy and an insufficiently favorable environment for doing business and innovations and, as a result, the low level of using digital technologies by business structures [3].

The use of information and telecommunication technologies, existing and functioning electronic services,

information systems, as well as portals of state and municipal services, should be carried out in order to simplify the implementation of citizens' rights. However, citizens cannot always exercise such rights in full. Thus, the Constitution of the Russian Federation considers the right to appeal as one of the most important ones of a citizen. A special category is complaints against decisions on cases of administrative offenses. Establishing the possibility of using digital technologies to bring citizens to administrative responsibility and sending them decisions on cases of administrative offenses, the administrative legislation, however, does not provide citizens with an equal opportunity to appeal against such decisions by sending an electronic complaint.

In terms of this fact, the Supreme Court of the Russian Federation has formulated the following legal position: within the meaning of the provisions entrenched in Chapter 30 of the Code of Administrative Offenses of the Russian Federation, a complaint against a decision on an administrative case should be filed in hard copy. However, this legal position directly contradicts, for example, the Instruction on the Organization of Consideration of Citizens' Appeals in the System of the Ministry of the Interior of the Russian Federation to the Order of the Ministry of Interior of Russia. According to Clause 1 of Article 4 of this Order, citizens may apply to the state authorities with complaints both in writing and in electronic form. However, the Russian Ministry of the Interior, referring to the above decision of the Supreme Court, refuse to accept complaints against decisions on cases of administrative offenses filed through the Internet information and telecommunication network without an enhanced qualified digital signature. The main argument is the inability to establish the identity of the applicant, which contradicts Parts 1, 1.1 of Article 30.1 of the Code of Administrative Offences of the Russian Federation. At the same time, applicants on civil cases without a digital signature may submit complaints and applications in electronic form, through a uniform identification and authentication system.

Being launched in the 21st century around the world, the process of "digitalization" continues developing rapidly, stimulating new changes and technological innovations, which, in turn, pose difficult legal problems in the digital ecosystem [4]. These include ensuring the safety of personal data on the Internet and cybersecurity, protecting digital rights of citizens and property from criminal infringement in the digital environment, intellectual rights and other constitutional rights of citizens, maintaining the legality of digital services, defending critical infrastructure and cloud information, as well as assuring privacy.

The beginning of a broad discussion about the digital paradigm and modern intellectual property was initiated by Jan Hargraves [5]. It was initiated in the coming digital era due to the specifics of protecting copyright and other rights in the digital space and in connection with the adoption by the United Kingdom of the Digital Economy Act 2010. Later, it was replaced by the new law of the same name of 2017, the UK Digital Economy Act 2017 [6], which expanded the rights of the supervising body in the field of IT communications (Ofcom) to monitor compliance with copyright and the jurisdiction of the courts in protecting copyright holders, Internet interests operators, and users of the Internet [7].

Along with the development of digital remote technologies and the growth of a huge number of electronic services, citizens is under the risk of becoming victims of criminals operating exclusively in the digital environment. Thus, knowing the user's login and password, it is possible to take easy control of other people's money, obtain a loan remotely, etc.

On 13 May 2017, the whole world was discussing the yesterday attack of unknowns on 200,000 computers in 150 countries. In fact, all of humanity was attacked. It is believed that the attack was stopped accidentally when two British programmers identified a nonexistent domain, which the virus was accessing, and registered a domain with that name, which turned out to be the "Stop the Spread of the Virus" command [8].

Every day, dozens of citizens' appeals to law enforcement agencies of the Russian Federation on the fact of unlawful acts against them in the field of the digital economy and the digital environment; particularly, criminals remotely steal citizens' funds from bank accounts. However, if the amount of theft is less than 2,500 rubles, it is not a criminal offense but it is considered only an administrative offense with a short term of bringing to administrative responsibility, 3 months (Article 7.27 of the Code of Administrative Offenses of the Russian Federation). In addition, as a part of the verification of the report on the offense, it is impossible to conduct a high-quality investigation, to send requests to specialized police information divisions in order to identify the offender.

More recently, for the first time in Russia, a criminal case was instituted on the fact of the purchase and sale of an apartment remotely, through an enhanced electronic signature without the knowledge of the owners of real estate. Only in September 2019, the title holder with enormous through a judicial proceedings was able to regain its electronically "stolen" apartment [9]. In this connection, a reasonable question arises, for what purpose the law on electronic signature has been adopted if it in no way protects a citizen without its personal presence?!

As the professor at Oxford University, the Swedish philosopher Nick Bostrom, justly noted. "We almost certainly live within a computer simulation." In online publications about the hypothesis of simulation, it is often possible to find mention of Barry Dayton, who, on the one hand, made attempts to justify that fact that humanity lived in simulation, and on the other, deduced ethical principles against the creation of simulations. Thus, it turns out that comprehensive digitalization only proves the simulation hypothesis [10].

II. RESEARCH METHODOLOGY

The methodological base of this study included general scientific methods of cognition, including the principle of objectivity, systemicity, induction, deduction, etc. Along with general scientific methods of cognition, the following private scientific methods were used: descriptive, linguistic, and comparative-legal. The study topic is disclosed from the standpoint of general scientific methods (sociological, systemic, structural-functional, concrete historical, and statistical); general logical methods of theoretical analysis, private scientific methods (comparative law, technical and legal analysis, concretization, and interpretation). The authors analyzed the materials of 50 criminal cases of economic nature committed using digital technology. Statistics and analytical data posted on the official websites of the Ministry of the Interior of Russia and the Judicial Department under the Supreme Court of the Russian Federation have been studied. The questioning method has been used to interview 150 respondents, including 52 employees of divisions of district authorized police officers of the Ministry of the Interior of Russia (which directly check reports on embezzlement of funds in the digital environment with damage up to 2,500 rubles).

III. RESULTS OF THE RESEARCH

Based on the results of our study, we came to the conclusion that the regulatory legal framework for the digital environment in the Russian Federation is in its infancy and needs close attention and updating on the part of all branches of power. The development of the legal framework for the digital economy and the digital environment in the Russian Federation is hindered by the following factors:

1. The growth of computer crime, including international crime;

2. The problem of ensuring human rights in the digital world, including the identification (correlation of a person with its digital image), the safety of the user's digital data, as well as the problem of ensuring citizens' trust in the digital environment;

3. Threats to society associated with trends in the construction of complex hierarchical information and telecommunication systems that widely use virtualization, remote (cloud) data storages, as well as heterogeneous communication technologies and terminal devices;

4. Enhancing the capabilities of the external information and technical impact on the information infrastructure, including critical information infrastructure;

5. The lag behind the leading foreign countries in the development of competitive information technologies;

The analysis of the criminal and administrative legislation also allows concluding that there are contradictions, forms and methods of investigation of criminal and administrative acts. In the latter case, taking into account the statute of limitations and methods of verification, it is practically impossible to establish the offender.

IV. DISCUSSION OF RESULTS

Analyzing international law, it is impossible to disagree with Ye.V. Gromov, who claims that the foreign law has taken the path of delimiting computer criminal acts depending on the sphere of public relations the criminal encroaches on [11]. These areas correspond to the criminological groups of computer crimes. The following three groups may be distinguished:

- economic computer crimes (the most common and dangerous crimes), for example, computer fraud;
- computer crimes against the rights and freedoms of individual entities and organizations that violate the inviolability of the private sphere, for example, illegal abuse of information on computer media, disclosure of information containing private, commercial secrets (information other than confidential nature should be on computer media); and
- computer crimes against the interests of the state and society as a whole, for example, disorganization of work of various systems (defense, energy, or gas supply), data changes during the counting of votes in elections, etc.

With the development of the electronic and digital space, criminal acts in the world of crime in the field of information technology, especially severe ones, are being committed more and more often. As the digitalization of the economy develops under conditions of social differentiation, we will have a decrease in traditional common crime, i.e., theft, robbery, plunder, or fraud. In the next ten years, new forms of unlawful infringements related to cybercrime will also spread. Cybercrimes and cybercriminals are becoming more sophisticated and violent. This is evidenced by the sharply increased number and risks of hacker attacks, leakage of personal information, and imitation of a person's appearance according to data from the social network. According to Group-IB, in 2018, cybercriminals attacked banks in the USA and the UK more than 20 times. It is almost impossible to track down such criminals. According to experts, the average damage from one such attack for the USA is 500 thousand dollars; 72 million rubles, for Russia. The number of cybercrimes has increased by 75%, as stated in the Digital Economy of the Russian Federation Program. According to the Russian Prosecutor General's Office, the number of cybercrimes in Russia in 2017 has six times increased compared to 2013 [12]. Given 66 thousand IT crimes recorded in 2017, this figure was only 11 thousand in 2013 [13].

V. CONCLUSIONS

Unfortunately, the striving of society to expand the scope of digital services includes both the comfort and the threat to digital (information) security. On the one hand, authorities in the Russian Federation prohibit filing complaints on administrative offenses in electronic form, and on the other, they allow selling apartments remotely through a public services portal, although the latter case significantly increases

the risk of unauthorized interference.

In order to strengthen information security and achieve a state of security of personality, society, and state from internal and external information threats, which ensure the execution of constitutional rights and freedoms of human and citizen, worthy quality and standard of living of citizens, sovereignty and sustainable socio-economic development of the Russian Federation in the context of the digital economy, the interested authorities, within the next ten years, will need the following:

- Ensuring the unity, stability, and security of the information and telecommunication infrastructure of the Russian Federation at all levels of the information space;
- Ensuring organizational and legal protection of personality, business, and state interests when interacting in the digital economy;
- Regulatory consolidation of a special type of administrative offense and crime, an act committed by means of information technology in a digital environment, which allows increasing the crime solution in this field.
- Adoption of amendments to the federal law allowing citizens and others to file complaints on administrative cases electronically, as the civil proceedings admits.
- Using exclusively Russian technologies in activities, ensuring integrity, confidentiality, authentication, and accessibility of the information being transmitted and its processing methods; and
- Applying information protection technologies using Russian cryptographic standards.

References

[1] Begishev I.R. Prestupleniya v sfere tsifrovoy informatsii / I.R. Begishev // Informatsionnoye pravo. - 2010. - № 2. - S. 18-21.

[2] Vagin, V.N., Derevyanko, A.V. & Kutepov, V.P. Sci. Tech. Inf. Proc. (2018) 45: 368. https://doi.org/10.3103/S014768821805009X

[3] Programma "Tsifrovaya ekonomika Rossiyskoy Federatsii" // «Finansovyy biznes». 2017. T. 6 (191). S. 3-10

[4] Hajli N. Social commerce and new development in e-commerce technologies / N. Hajli, M.S. Featherman // International Journal of Information Management. - 2017. - № 37. - P. 177-178.

[5] Ian Hargreaves. Digital Opportunity: A Review of Intellectual Property and Growth. London: HM Government, 2011. C. 53: http://www.ipo.gov.uk/ipreview-finalreport.pdf. (data obrashcheniya 01.09.2019 g.).

[6] Digital Economy Act, 2017: http://www.legislation.gov.uk/ukpga/2017/30/pdfs/ukpga_20170030_en.pdf. (data obrashcheniya 01.09.2019 g.).

[7] Mastering the Digital Imperative. Digital BCG, 2017. https://www.bcg.com/expertise/digital-bcg/default.aspx. (data obrashcheniya 01.09.2019 g.).

[8] NHS cyberattack: Seven trusts still turning away patients // https://news.sky.com/story/europol-warns-of-further-cyberattacks-on-monday-morning-10876985

[9] Elektronnaya podpis' ostavila bez kvartiry // https://www.kommersant.ru/doc/3969174

[10] Bozeman b.1, Anderson d.m. Arizona State University, Phoenix public policy and the origins of bureaucratic red tape: implications of the Stanford yacht scandal // Administration & Society, 2016. 6 (48). s. 736-759

[11] Gromov Ye.V. Razvitiye Ugolovnogo Zakonodatel'stva O Prestupleniyakh V Sfere Komp'yuternoy Informatsii V Zarubezhnykh Stranakh (SSHA, Velikobritanii, FRG, Niderlandakh, Pol'she) // Vestnik Tomskogo gosudarstvennogo pedagogicheskogo universiteta. 2006.№ 11 (62). S. 30-35.

[12] Khakerskaya gruppirovka MoneyTaker opustoshayet banki SSHA i Rossii // URL: https://newdaynews.ru/technology/622809.html.

[13] Aliyev V.M. Politiko-pravovyye aspekty perekhoda k tsifrovoy ekonomike v Rossii // Rossiyskiy sledovatel'. 2018. N 9. S. 48 - 52.