Как цитировать: Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 5. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 380 с. EDN: BVPNNQ. DOI: http://dx.doi.org/10.21202978-5-8399-0818-5_5_380

For citation: Digital Technologies and Law: collection of scientific articles of the II International Scientific and Practical Conference (Kazan, 2023, September 22) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 5. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2023. – 380 p. EDN: BVPNNQ. DOI: http://dx.doi.org/10.21202/978-5-8399-0818-5_5_380

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
II Международной научно-практической конференции

22 сентября 2023 г.
г. Казань

В шести томах
Том 5

Казань ■ КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ■ 2023

DIGITAL TECHNOLOGIES AND LAW

Collection of scientific articles
of the II International Scientific and Practical Conference

2023, September 22
Kazan

In 6 volumes
Volume 5

Kazan ■ KIU "POZNANIYE" PUBLISHERS ■ 2023

УДК 004:34(063)
ББК 67с51я43
Ц75

Печатается по решению редакционно-издательского совета
Казанского инновационного университета имени В. Г. Тимирясова

Ц75 Цифровые технологии и право: сборник научных трудов II Международной научно-практической конференции (г. Казань, 22 сентября 2023 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 5. – Казань: Изд-во «Познание» Казанского инновационного университета, 2023. – 380 с. EDN: BVPNNQ. DOI: http://dx.doi.org/10.21202/978-5-8399-0818-5_5_380
ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0818-5 (Том 5)

Вошедшие в сборник научные труды приурочены к II Международной научно-практической конференции «Цифровые технологии и право», состоявшейся 22 сентября в Казани в рамках Международного форума Kazan Digital Week 2023, организуемого Правительством Российской Федерации совместно с Кабинетом Министров Республики Татарстан.

Широкий круг рассмотренных на конференции теоретико-методологических и практико-ориентированных, междисциплинарных и отраслевых вопросов связан с приоритетами правового развития цифровых технологий, нормативным регулированием цифровой среды, перспективами правового воздействия на формирующиеся и новые общественные отношения, когнитивно-поведенческие паттерны в условиях цифровизации и алгоритмизации социального программирования, автоматизированного принятия правовых решений операционно-интеллектуальными системами, доминирования цифровых платформ на цифровом рынке, технологических инноваций и многим другим.

Научные труды представленного тома систематизированы по современным трендам развития цифровых технологий в системе международно-правовых, частноправовых (цивилистических), трудовых и связанных с ними отношений.

Нашедшие отражение в многотомном издании идеи и предложения в своей совокупности являются ключом к пониманию интеллектуальной карты смыслов, которые будут интересны ученым-правоведам и экспертам в области цифровых технологий, практикующим юристам, представителям правотворческих и правоприменительных органов, государственным служащим и участникам реального сектора экономики, включая разработчиков и производителей продуктов достижений цифровых технологий, молодым исследователям-студентам, магистрантам и аспирантам, всем интересующимся вопросами взаимовлияния цифровых технологий и права.

УДК 004:34(063)
ББК 67с51я43

ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0818-5 (Том 5)

UDC 004:34(063)
LBC 67c51я43

Published by the decision of the Editorial-Publishing Board
of Kazan Innovative University named after V. G. Timiryasov

Digital Technologies and Law: collection of scientific papers of the II International Scientific and Practical Conference (Kazan, 2023, September 22) / I. R. Begishev, E. A. Gromova, M. V. Zaloilo, I. A. Filipova, A. A. Shutova (Eds.). In 6 vol. Vol. 5. – Kazan: Poznaniye Publishers of Kazan Innovative University, 2023. – 380 p. EDN: BVPNNQ. DOI: http://dx.doi.org/10.21202/978-5-8399-0818-5_5_380
ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0818-5 (Vol. 5)

The scientific works included in the collection are timed to coincide with the II International Scientific and Practical Conference "Digital Technologies and Law", held on September 22 in Kazan as part of the International Forum "Kazan Digital Week 2023", organized by the Government of the Russian Federation jointly with the Cabinet of Ministers of the Republic of Tatarstan.

A wide range of theoretical, methodological and practice-oriented, interdisciplinary and sectoral issues discussed at the conference are related to the priorities of the legal development of digital technologies, regulatory regulation of the digital environment, prospects for legal influence on emerging and new social relations, cognitive-behavioral patterns in the context of digitalization and algorithmization of social programming, automated legal decision-making by operational-intelligent systems, the dominance of digital platforms in the digital market, technological innovation and much more.

The scientific works of the presented volume are systematized according to modern trends in the development of digital technologies in the system of international legal, private law (civil law), labor and related relations.

The ideas and proposals reflected in the multi-volume publication in their entirety are the key to understanding the intellectual map of meanings that will be of interest to legal scholars and experts in the field of digital technologies, practicing lawyers, representatives of law-making and law enforcement bodies, government officials and participants in the real sector of the economy, including developers and manufacturers of products of digital technology achievements, young student researchers, undergraduates and graduate students, everyone interested in the mutual influence of digital technologies and law.

UDC 004:34(063)
LBC 67c51я43

ISBN 978-5-8399-0820-8
ISBN 978-5-8399-0818-5 (Vol. 5)

S. M. Díaz,
student,
University of Sancti Spíritus «José Martí Pérez»

WEB SCANNER: A VULNERABILITY DETECTION TOOL TO SCAN A WEBSITE GIVEN ITS URL

Abstract. Information constitutes a very important asset for people or organizations, therefore, protecting it has become a priority for everyone, unfortunately there is not a unique formula that grantees a complete and total protection to the information. With that in mind, it becomes necessary the use of a software that provides help and facilitates work for the cybersecurity specialists so they can provide the best possible protection of data. Objective: Develop a system that can scan a given URL link of a website, and provide all the necessary information about the site. Methods: From a scientific point of view, the scientific observation, document analysis, survey and interview are considered as methods, giving place to a susceptible proposal to the scientific verification and validation. Results: The implementation of a website that contains a vulnerability detection system (web scanner), which can scan a website given its URL. Conclusions: the implementation of the said system for the security of the information in the University of Sancti Spíritus «José Martí Pérez» (UNISS) is valued as a positive support for the security against phishing attacks, in a single repository.

Keywords: cybersecurity, information, malware, phishing attacks, social engineering, tool, vulnerability analysis, web scanner

ВЕБ-СКАНЕР: СРЕДСТВО ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ДЛЯ СКАНИРОВАНИЯ ВЕБ-САЙТА ПО ЕГО URL-АДРЕСУ

Аннотация. Информация представляет собой очень важный актив для людей или организаций, поэтому ее защита стала приоритетной задачей для всех, но, к сожалению, не существует уникальной формулы, обеспечивающей полную и абсолютную защиту информации. В связи с этим возникает необходимость в использовании программного обеспечения, которое помогает и облегчает работу специалистов по кибербезопасности, чтобы они могли обеспечить наилучшую защиту данных. Целью исследования стала разработка системы, способной сканировать заданную URL-ссылку сайта и предоставлять всю необходимую информацию о нем. С научной точки зрения в качестве методов рассматриваются научное наблюдение, анализ документов, анкетирование и интервьюирование, уступающие место восприимчивому предложению, подлежащему научной проверке и обоснованию. В результате был создан веб-сайт, содержащий систему

обнаружения уязвимостей (веб-сканер), которая может сканировать веб-сайт по его URL-адресу. Внедрение указанной системы для защиты информации в Университете Санкти-Спиритус «Хосе Марти Перес» оценивается как эффективная поддержка защиты от фишинговых атак в едином хранилище.

Ключевые слова: кибербезопасность, информация, вредоносное ПО, фишинговые атаки, социальная инженерия, инструмент, анализ уязвимостей, веб-сканер

Introduction. Cybersecurity is one of the leading niches of information technology. It refers to the tools, frameworks, techniques, and practices implemented to ensure the security of computing, information, and other systems and their users.

Cybersecurity covers the broad range of technical, organizational and governance issues that must be considered to protect networked information systems against accidental and deliberate threats. It goes well beyond the details of encryption, firewalls, anti-virus software, and similar technical security tools. This breadth is captured in the widely used International Telecommunication Union (ITU) definition [7].

The importance of cybersecurity has increased as so many government, business, and day-to-day activities around the world have moved online. But especially in emerging economies, "[m]any organizations digitizing their activities lack organizational, technological, human resources and other fundamental ingredients needed to secure their system, which is the key for the long-term success [2, 7].

With the dawn of the World Wide Web, installing antivirus software was necessary to protect your computer from attacks. Even though destructive assaults back then were not as well known, as they are today, the history of cyber security threats has kept pace with the advancement in information technology.

Since computers were connected to the internet and began exchanging messages, cybercrime has substantially changed. Even if the amount of risk is substantially higher now than it was back then, computer users have been understandably concerned about these threats for a long time.

Despite the fact that the Internet has positively affected people's lives, there are negative issues emerged related to the use of Internet. Cases like cyber-bully; online fraud, racial abuse, pornography and gambling had increased tremendously due to the lack of awareness and self-mechanism among Internet users to protect themselves from being victims to these acts. However, past research revealed that the level of awareness among Internet users is still low or moderate. One of the vital measures to be taken is to cultivate knowledge and awareness among Internet users from their early age, i.e., young children. Young children specifically, need to be educated to operate in a safe manner in cyberspace and to protect themselves in the process [6].

Cybercrime against children and adolescents is certainly a concern for parents, as they sometimes do not realize their child is a victim of cybercrime. Many parents are unaware of the activities their children perform in cyberspace. Some children are bullied through comments and insults; they may also be intimidated, harassed, abused or sexually exploited [6].

Cyber risks could change as technology develops. Cybercriminals are always developing new ways to access systems and steal data.

Therefore, an educated workforce is essential to building trustworthy systems. Yet, issues about what should be taught and how are being ignored by many of the university faculty who teach cybersecurity courses a problematic situation [2].

Unfortunately, cybercriminals or "Hackers" are always one-step ahead of cybersecurity specialists in the sense that they are always developing ways to surpass the obstacles developed by the cybersecurity specialists, and always developing new tools to violate the information security policies and measures.

The word «hacker» conjures the image of someone with ill intent toward individuals, websites, and company information systems. The prevailing theory is they look for ways to mine company data and destroy or change customer information. Those types of «bad guys» certainly exist – the cybersecurity industry calls them Black Hats, but in reality, they are not the only hackers lurking in cyberspace.

Over time, cybersecurity specialists came up with a way to become one-step above the hackers called "Ethical Hacking", which is hacking ethically to learn the vulnerabilities of a system.

There is a technique in ethical hacking called "Thinking like a hacker", which means to be able to learn how to defend a system first one needs to learn how to attack it, the best practice to achieve the best possible security is by thinking as a hacker and asking the question "What would the hacker do?".

Hackers can be sorted in varies categories, the most popular ones are "Black Hat Hackers" and "White Hat Hackers":

Black Hat hackers are criminals who break into computer networks with malicious intent. They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information.

White hat hackers or ethical hackers is an individual who uses hacking skills to identify security vulnerabilities in hardware, software or networks. However, unlike black hat hackers white hat hackers respect the rule of law as it applies to hacking.

With the rapidly increasing prominence of information technology in recent decades, various types of security incidents, such as unauthorized access, distribution denial of service (DDoS), malware attack, zero-day attacks, data breaches, social engineering or phishing, etc., have increased at an exponential rate in the last decade [1].

Social engineering attacks aim at tricking individuals or enterprises into accomplishing actions that benefit attackers or providing them with sensitive data such as social security number, health records, and passwords.

Social engineering attacks are multifaceted and include physical, social and technical aspects, which are used in different stages of the actual attack [3].

Physical approaches:

As the name implies, physical approaches are those where the attacker performs some form of physical action in order to gather information on a future victim. This can range from personal information (such as social security number, date of birth) to valid credentials for a computer system [4].

Social approaches:

The most important aspect of successful social engineering attacks are social approaches. Hereby attackers rely on socio-psychological techniques such as Cialdini's principles of persuasion to manipulate their victims [4].

Technical approaches:

Technical attacks are mainly carried out over the Internet. Granger notes that the Internet is especially interesting for social engineers to harvest passwords, as users often use the same (simple) passwords for different accounts [5].

Social engineering is one of the biggest challenges facing network security because it exploits the natural human tendency to trust [3].

Although social engineering is a technique, it contains a very big amount of attacks in its categories and one of the most famous and used attacks in these categories are the phishing attacks, which is when attackers attempt to trick users into doing 'the wrong thing', such as clicking a bad link that will download malware, or direct them to a dodgy website.

It is thought that the first phishing attacks happened in the mid-1990s, when a group of hackers posed as employees of AOL (America Online) and used instant messaging and email to steal users' passwords and hijack their accounts.

The focus of this paper is directed to the utility that the web scanner will provide the users and cybersecurity specialists of the University of Sancti Spíritus "José Martí Pérez" and how can they avoid being victims of a phishing attack. Since this tool will, show all the information related to a web site or a URL.

Theatrical framework

The advancements in digital communication technology have made communication between humans more accessible and instant. However, personal and sensitive information may be available online through social networks and online services that lack the security measures to protect this information. Communication systems are vulnerable and can easily be penetrated by malicious users [2]. The last few years has seen a rise in the frequency with which people have conducted meaningful transactions online; from making simple purchases to paying bills to banking, and even to getting a mortgage or car loan or paying their taxes. This rise in online transactions has unfortunately been accompanied by a rise in attacks [4, 8].

In this paper will be treating a computer software under development called a web scanner, which as the name indicates it scans a website given its URL. This project started with a thesis on cybersecurity management in the University of Sancti Spíritus "José Martí Pérez" for the department of cyber and information security.

Importance of the web scanner

Every organization, institution, University, company…etc. has a cybersecurity department that keeps all the information whether its personal or work related safe and protected, that being said the cybersecurity specialists need tools and software to facilitates the work.

The University of Sancti Spíritus "José Martí Pérez" is not the exception, in the university there is a cybersecurity department in need of a software that can make the control and monetarization easier.

In said university, most of the attacks they suffer from are categorized as social engineering, specifically phishing attacks to the members of all the faculties, students, teachers and employees.

That being said a software like the web scanner proposed in this paper is a very helpful tool for the department and for the members of the university, that way whenever there is a suspicious email sent to any member that contains an URL can be scanned to know what that URL hides. Which makes the web scanner a very important addition to the department, that way they can limit all the phishing attacks in the university.

Methods. The methodology used allowed obtaining a flexible proposal as an alternative solution, susceptible to scientific verification; for this paper were used the following scientific research methods:

From a theoretical point of view:

Historical-logical analysis that allowed the study of the ways in which the standards and norms of cybersecurity have evolved.

Analytical-synthetic analysis, which made it possible to study the main cybersecurity systems, as well as vulnerability detection ways and systems.

From an empirical point of view:

Observation, which guided the study of the state of the art, allowing a systemic, selective and objective analysis of the main systems that can currently carry out vulnerability detection systems.

Unstructured interview, which was applied with the intention of obtaining information regarding vulnerability detection, processes, as well as expert criteria on the subject matter.

Results. The processing of the results obtained with the application of the methods described, allowed to identify the methodologies and tools to develop the system for the vulnerability detection system (Web Scanner) of cybersecurity of the University of Sancti Spíritus «José Martí Pérez», which are presented next.

For the development of the web scanner, the following technologies were chosen:

Python: Python is a programming language widely used in web applications, software development, data science, and machine learning (ML). One of the reasons that Python programming language was chosen because it contains many libraries for cybersecurity development.

Linux OS: Linux is a Unix-like, open source and community-developed operating system (OS) for computers, servers, mainframes, mobile devices and embedded devices. It is supported on almost every major computer platform, including x86, ARM and SPARC, making it one of the most widely supported operating systems.

The system works based on a given URL and once it has provided it can scan it showing the following results:

IP address: An IP is an internet protocol address. Essentially, it is a numeric value assigned to a network device, and it is used for the identification and location of a network device. IP addresses are assigned to every type of network device.

An IP address consists of a series of four numbers (each between 0 and 255) separated by periods. For example, an IP address might look like this: 192.168.0.1.

There are two types of IP addresses: IPv4 and IPv6. IPv4 addresses are the older and more common type of IP address, consisting of 32 bits (4 bytes) and allowing for approximately 4.3 billion unique addresses. IPv6 addresses are the newer type of IP address, consisting of 128 bits (16 bytes) and allowing for a virtually unlimited number of unique addresses.

IP addresses are used for a variety of purposes, including:

Identifying devices on a network: IP addresses are used to uniquely identify devices on a network, such as computers, smartphones, servers, printers, and routers.

Routing internet traffic: routers to route internet traffic between devices on different networks use IP addresses. When a device sends data to another device over the internet, the data is divided into packets and sent to the destination device's IP address.

Geo-location: IP addresses can be used to determine the geographic location of a device. This information can be used for various purposes, such as targeted advertising or content delivery.

Network security: IP addresses are used in network security to identify potential threats, such as spam, malware, or unauthorized access attempts. By analyzing the IP addresses of incoming network traffic, security professionals can identify and block potential threats.

Network administration: network administrators to manage and configure network devices, such as routers and switches, use IP addresses. By assigning unique IP addresses to each device, administrators can manage the devices remotely and troubleshoot network issues.

Domain name: A domain name is a string of text that maps to an alphanumeric IP address, used to access a website from client software. In plain English, a domain name is the text that a user types into a browser window to reach a particular website.

Domain names are made up of two or more parts, separated by periods. The rightmost part of the domain name is called the top-level domain (TLD) and identifies the type of organization or country associated with the domain. For example, «.com» is a common TLD that stands for «commercial», while «.org» stands for «organization». Other common TLDs include «.net», «.edu», and «.gov»…etc.

The part of the domain name to the left of the TLD is known as the second-level domain (SLD) and is chosen by the website owner. For example, in the domain name «google.com», «google» is the SLD and «.com» is the TLD.

Domain names are used for a variety of purposes, including:

Identifying websites: Domain names are used as a human- readable and memorable way to identify websites on the internet. Instead of having to remember a website's IP address (a string of numbers); users can simply type in the website's domain name to access it.

Branding: Domain names are often used as part of a company's branding strategy, helping to create a memorable and recognizable online presence.

Email: Domain names are also used to identify email addresses. For example, the email address «john.doe@example.com» is associated with the domain name «example.com».

SEO: Domain names can also affect a website's search engine optimization (SEO) by influencing its relevance and authority in search engine rankings.

Reselling: Domain names can be bought and sold like other forms of digital assets, and some people make a business out of buying and selling domain names.

Nmap scan: Nmap, short for Network Mapper, is a free and open source tool used for vulnerability checking, port scanning and, of course, network mapping.

Nmap scan is one of the most popular network scanning tools available and is widely used by system administrators, security professionals, and network engineers.

Nmap works by sending specially crafted packets to target hosts and analyzing their responses. The tool can be used to perform a variety of tasks, such as:

Host discovery: identifying hosts that are active on a network

Port scanning: identifying open ports on a target host

Service and version detection: identifying the services running on open ports and their version numbers

Operating system detection: identifying the operating system running on a target host

Vulnerability scanning: identifying potential vulnerabilities on a target host

Nmap provides a variety of options and parameters that allow users to customize their scans and obtain results that are more detailed. It also includes a scripting engine that allows users to write custom scripts to perform more advanced scans and tasks.

Robots.txt: The robots.txt file is a text file that is placed in the root directory of a website to provide instructions to web robots (also known as web crawlers or spiders) on how to crawl and index the website's pages. The robots.txt file is an optional file, and not all websites have one.

The main purposes of the robots.txt file are:

To control which pages on the website should be crawled and indexed by search engines: The robots.txt file can be used to prevent search engines from indexing certain pages on a website. This can be useful if there are pages on the website that the website owner does not want to appear in search engine results (such as test pages or pages with sensitive information).

To prevent web crawlers from overloading the website: Web crawlers can consume a lot of bandwidth and resources, which can slow down or overload a website. The robots.txt file can be used to limit the frequency and depth of crawling by web robots to prevent this from happening.

To protect private or confidential information: The robots.txt file can be used to prevent web robots from crawling and indexing pages that contain private or confidential information (such as login pages or user profiles).

Whois scan: A WHOIS search will provide information regarding a domain name, such as example.com. It may include information, such as domain ownership, where and when registered, expiration date, and the name servers assigned to the domain.

WHOIS scan is a type of network reconnaissance that involves querying a WHOIS database to obtain information about a domain name or IP address. The WHOIS database contains information about the ownership and administrative contacts for a particular domain name or IP address, as well as other details such as the registration and expiration dates.

WHOIS scans can be performed using various online tools and services, as well as with command-line utilities such as whois on Linux/Unix operating systems.

Some of the common use cases for WHOIS scans:

Domain name registration information: WHOIS scans can be used to obtain information about the owner of a domain name, as well as the organization responsible for registering and managing the domain. This information can be useful for investigative purposes or for contacting the domain owner or administrator.

IP address ownership information: WHOIS scans can also be used to obtain information about the owner of an IP address block. This information can be useful for identifying the organization responsible for a particular network or for investigating potential abuse or security incidents.

Network reconnaissance: WHOIS scans can be used as part of a larger network reconnaissance effort to gather information about a target organization's infrastructure and digital footprint. The information obtained from WHOIS scans can be used to identify potential attack vectors or vulnerabilities.

Brand protection: WHOIS scans can be used by organizations to monitor and protect their brand names and trademarks. By regularly querying the WHOIS database for domain names containing their brand names or trademarks, organizations can identify potential cases of cybersquatting or trademark infringement.

After knowing all that information about a given URL, it becomes an easy task to identify a phishing attack, which makes it a very useful and important tool for the department.

Conclusions. Cybersecurity now a day is one of the most important subjects around the world, since all the information whether it was personal, professional or work related is online, the need of security systems to prevent the loss of said information is something highly important and necessary.

The web scanner is a tool that have been around for years and it does a great work preventing phishing attacks victims to fall into the trap, which makes it a very necessary and important tool for every institution, organization, university and company.

With the help of the web scanner, it is predicted to decrease the number of victims of a social engineering phishing attack in the University of Sancti Spíritus "José Martí Pérez".

References

1. Ahsan M., Nygard K. E., Gomes R., Chowdhury M. M., Rifat N., Connolly J. F. Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning a Review // Journal of Cybersecurity and Privacy. 2022. № 2. Pp. 527–555.

2. Gromova E. A., Petrenko S. A. Quantum Law: The Beginning // Journal of Digital Technologies and Law. 2023. Vol. 1(1). Pp. 62–88.

3. Krombholz K., Hobel H., Huber M., Weippl E. Advanced social engineering attacks// Journal of Information Security and Applications. 2015. № 22. Pp. 113–122.

4. Rahman N. A., Sairi I. H., Zizi N. A., Khalid F. The Importance of Cybersecurity Education in School // International Journal of Information and Education Technology. 2020. № 10. Pp. 378–382.

5. Ramzan Z. Phishing Attacks and Countermeasures // Handbook of Information and Communication Security / P. Stavroulakis & M. Stamp (Eds.). 2010. Pp. 433–448.

6. Salahdine F., Kaabouch N. Social Engineering Attacks: A Survey // Future Internet. 2019. № 11. Pp. 89–92.

7. Schneider, F. B. Cybersecurity Education in Universities // IEEE Security & Privacy. 2013. Vol. 11. Pp. 3–4.

8. Veale M., Brown I. Cybersecurity // Internet Policy Review. 2020. Vol. 9. Pp. 1–22.

L. A. Quintero-Domínguez,
PhD, Associate Professor,
University of Sancti Spíritus «José Martí Pérez»
J. A. Antón Vargas,
MSc, Assistant Professor,
University of Sancti Spíritus «José Martí Pérez»
S. Pérez Madrigal,
Eng., Instructor,
University of Sancti Spíritus «José Martí Pérez»

WRAPPER ALGORITHM FOR MULTI-INSTANCE LEARNING: EARLY RESULTS

Abstract. Multi-instance learning is a generalization of supervised learning, where each example is represented by a labeled bag composed by a set of instances. Several multi-instance learning methods transform each bag into a single instance and then apply standard supervised learning methods. This paper presents a new multi-instance learning method that transforms the multi-instance data and is inspired by text mining. The proposed method transforms the multi-instance data into a traditional attribute-value representation by creating a corpus of documents formed by artificial words to reduce the loss of information during the transformation process. In addition, the proposed method was empirically evaluated using nine multi-instance datasets and two learning methods that transform the multi-instance data into a traditional attribute-value representation. The empirical study indicates that, in terms of classification accuracy, the proposed method is competitive with the learning methods used in the comparison.

Keywords: Multi-instance learning, Bag-of-words, Wrapper method, data, algorithm, learning, learning methods

АЛГОРИТМ «ОБЕРТКИ» ДЛЯ МНОГООБЪЕКТНОГО ОБУЧЕНИЯ: ПЕРВЫЕ РЕЗУЛЬТАТЫ

Аннотация. Многофакторное обучение – это обобщение супервизорного обучения, в котором каждый пример представлен меченым мешком, состоящим из множества экземпляров. Некоторые методы многофакторного обучения преобразуют каждый мешок в один экземпляр и затем применяют стандартные

методы обучения с супервизией. В данной работе представлен новый метод многоэкземплярного обучения, который преобразует многоэкземплярные данные и вдохновлен разработкой текстов. Предлагаемый метод преобразует многоинстанционные данные в традиционное представление «атрибут-значение» путем создания корпуса документов, сформированного из искусственных слов, чтобы уменьшить потерю информации в процессе преобразования. Кроме того, была проведена эмпирическая оценка предложенного метода на девяти многофакторных наборах данных и двух методах обучения, преобразующих многофакторные данные в традиционное представление «атрибут-значение». Эмпирическое исследование показало, что по точности классификации предложенный метод конкурентоспособен с использованными в сравнении методами обучения.

Ключевые слова: многофакторное обучение, метод «обертки», данные, алгоритм, обучение, методы обучения

Introduction. Multi-instance learning is a generalization of standard propositional learning, also called attribute-value learning. While in standard learning an instance is represented by a fixed-size vector of attribute-value pairs that has a class label associated with it, in multi-instance learning an instance is represented by a bag of attribute-value vectors and the class label is associated with the whole bag.

Multi-instance learning has attracted increasing interest primarily because of the wide variety of real-world problems that can be modeled quite naturally as multi-instance problems. These problems include text classification [1] image retrieval and classification [3, 4] prediction of pharmacological activity [3], index web page recommendation [5] and prediction of academic performance [6].

Since the introduction of multi-instance learning, the number of multi-instance classification methods has grown considerably. Many authors have proposed categories to try to capture the distinctive features of these methods [1]. Recently [5] proposed three main categories:

Instance-based methods: these are algorithms where the learning process occurs at the instance level.

Bag-based methods: includes sorters that work directly in the bag space.

Mapping-based methods (wrappers): these are classifiers that apply a transformation to the data of the multi-instance problem so that traditional supervised learning algorithms can be applied to obtain the solution.

There are methods belonging to the wrapper category that transform multi-instance problems into traditional learning problems by replacing each bag with an attribute vector consisting of a summary statistic derived from the instances in the bag. These methods can lead to information loss when transforming the original multi-instance problems, which affects the classification efficiency.

Here we present a multi-instance learning method belonging to the category of mapping-based ones. The proposed method, called MIBoW, is inspired by text mining techniques and other fields where bag-of-words representation has been used [1–8]. MIBoW aims to achieve a reduction of information loss during the transformation of multi-instance data into a traditional attribute-value representation. MIBoW can be seen

as a transformation of the multi-instance dataset into a corpus of documents, where each bag becomes a document described by a set of artificial words that will be the attributes in the transformed dataset.

This paper shows the initial experimental evaluation performed to assess the effectiveness of the proposed method, where nine datasets and two mapping-based multi-instance learning methods were used. The experimental results indicate that the proposed method is competitive with the learning methods used.

Methodology. This section gives a brief introduction to multi-instance learning, presents the proposed method and describes the experimental study conducted.

Multi-instance classification. In multi-instance classification, a training example is a bag that contains multiple instances described by attribute-value vectors and has a single class label associated with it. Formally, in multi-instance classification, an example is a pair (X, y), where $X = \{x_1, \dots x_T\} \in N^x$ is a multi-set (bag) of T instances and $y \in Y$ is the class label of the instance. A bag is defined as a multiset $X \in N^x$ because multiple copies of the same instance may be included in a bag. The instances $x_i \in X (i = 1, \dots, T)$ are vectors of the m-space formed by the vector product of the m attributes describing the instances and Y is the set of class labels. The multi-instance classification task is to find a function $H : N^X \longrightarrow Y$ that, from a training set $D = \{(X_1, y_1), \dots, (X_T, y_T)\}$, allows to predict the class of a previously unseen example.

Multi-instance classification methods generally assume the existence of some relationship between the instances and the class label of the bag. This relationship is referred to as the multi-instance hypothesis. There are now a variety of multi-instance hypotheses that have been introduced as new solution methods for multi-instance problems have been developed [9]. The first hypothesis that was employed to define multi-instance learning was the standard [10].

The standard hypothesis states that a bag will be positive if and only if it contains any positive instances. That is, if the bag is negative all its instances will be negative, if the bag is positive at least one of its instances will be positive. Formally, given a function h, capable of estimating the class labels of an instance, the standard hypothesis can be described as:

$$H(X) = \bigvee_{x_i \in X} h(x_i)$$

MIBoW Method. This section describes the main steps of the MIBoW method. First, a transformation of the multi-instance dataset into a corpus of documents represented in the Bag-of-Words (BoW) format is performed. Each bag of instances is transformed into a textual document described by artificial words, which are constructed by combining the attribute names with their value: [attribute name]_[attribute value]. It should be noted that the attributes need to be discretized beforehand, so that the numerical values do not cause the generation of an excessive number of artificial words. The proposed method goes through each instance of the bag and generates the artificial words with each of the attributes, to form the set of words that will form the document corresponding to the bag.

Then, attribute-value pair vectors are constructed to represent the bags of the original multi-instance representation. For this, each of the artificial words that were generated in the corpus of documents is considered as an attribute in the new representation. The value associated to each document (example) for a word (attribute) is the frequency with which that word occurred in the document. The document is then associated with the same class label as the bag it represents.

Finally, after transforming the multi-instance dataset to the new attribute-value representation, a traditional learning algorithm is trained that will obtain a model capable of classifying a previously unseen bag after being transformed to the new representation.

Experimental study setup. This section presents the initial experimental study conducted to evaluate the effectiveness of the proposed method. For this purpose, nine multi-instance data sets were used, which are described in Table 1. For comparison, in addition to the proposed algorithm, two multi-instance learning methods were employed, which, like MIBoW, perform a transformation of the data to a traditional attribute-value representation: SimpleMI [11] and MIWrapper [12].

Table 1 Characteristics of the data sets used in the experimentation

Dataset	Attributes	Positive bags	Negative bags	Total bags
AntDrugs5	5	198	202	400
Atoms	10	125	63	188
24	24	125	63	188
Corel01vs02	9	100	100	200
Corel02vs03	9	100	100	200
Corel03vs04	9	100	100	200
Corel04vs05	9	100	100	200
EastWest	24	10	10	20
TREC9Sel-1	299	200	200	400

The proposed method, as well as SimpleMI and MIWrapper transform the multi-instance datasets to an attribute-value representation and then use traditional classification methods. For this reason, the experimental comparison was performed using the base classifiers RandomForest and SMO.

The Weka tool was used to perform the experimental evaluation and the measure used to measure the effectiveness of the methods was the classification accuracy. In addition, the data sets were discretized using the subdivision of the rank of each attribute into 10 intervals of equal length. The learning methods were used with the default parameter values of Weka.

Results and discussion. As mentioned above, the experimental study compared the proposed MIBoW method with the SimpleMI and MIWrapper methods. These methods have to be used in combination with a traditional classification algorithm as they transform the multiinstance data to a traditional attribute-value representation. RandomForest and SMO were used for this purpose.

Table 2 Experimental Evaluation Results (RF-RandomForest)

Dataset	RandomForest			SMO		
	MIBoW-RF	SimpleMI-RF	MIWrapper-RF	MiBoW-SMO	SimpleMI-SMO	MIWrapper-SMO
AntDrugs5	72.25	58.50	71.75	69.25	60.00	71.25
Atoms	79.71	66.49	66.49	68.71	66.49	66.49
Chains	89.36	73.42	77.63	84.56	77.19	69.62
Corel01vs02	84.50	70.00	86.00	87.00	72.50	82.50
Corel02vs03	81.00	75.00	80.00	84.00	74.00	71.50
Corel03vs04	95.50	90.00	88.50	94.00	90.00	74.00
Corel04vs05	100.00	99.00	95.50	100.00	98.50	90.00
EastWest	80.00	70.00	65.00	70.00	80.00	60.00
TREC9Sel-1	73.50	50.25	78.50	82.50	50.25	75.00

The Table 2 shows the results of the experimental evaluation in terms of classification accuracy. Analyzing the combinations with RandomForest, it can be seen that MIBoW obtains the best classification accuracy value in seven out of nine data sets. Additionally, to test whether these differences are statistically significant, statistical tests were performed following the methodology proposed by [10, 11] to compare several classifiers on several data sets. The Figure 1 shows the comparison between combinations with RandomForest using Friedman's test and Shaffer's procedure for the post hoc analysis with a value of $\alpha = 0.05$. In this figure it can be seen that the combination with MIBoW is significantly superior to those with SimpleMI and MIWrapper.

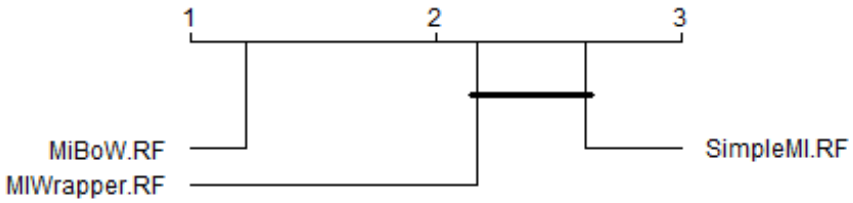

Figure 1. Comparation using RandomForest

Analyzing the combinations with SMO, it can be seen that MiBoW also obtains the best classification accuracy value in seven of the nine data sets. Similar to the methodology followed with the RandomForest combinations to test whether these differences are statistically significant, we used Friedman's test and Shaffer's procedure for the post hoc analysis with a value of $\alpha = 0.05$. In the Figure 2 it can be seen that the combination with MIBoW obtained first place in the Friedman ranking and is significantly superior to those with SimpleMI and MIWrapper.

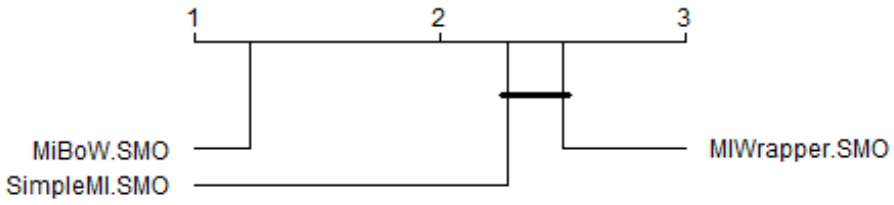

Figure 2. Comparison using SMO

Conclusion. In this paper, a new mapping-based multi-instance learning method, called MIBoW, is presented. The proposed method is inspired by text mining techniques, in particular the Bag-of-Words representation. MIBoW transforms multi-instance data into a traditional attribute-value representation by creating a corpus of documents consisting of artificial words to reduce information loss during the transformation process. The experimental study conducted indicates that, in terms of classification accuracy, the proposed method is superior to other methods that transform multi-instance data into an attribute-value representation.

As future work, it is planned to explore the effect of using typical text mining word weighting methods such as TF-IDF. In addition, it is intended to increase the experimental study using other learning methods and multi-instance datasets, to explore in more detail the advantages and possible limitations of MIBoW.

References

1. Amores J. Multiple instance classification: Review, taxonomy and comparative study // Artificial Intelligence. 2013. № 201. Pp. 81–105.

2. Chen Y., Bi J., Wang J. Z. MILES: Multiple-instance learning via embedded instance selection // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2006. Vol. 28. Pp. 1931–1947.

3. Demšar J. Statistical Comparisons of Classifiers over Multiple Data Sets // Journal of Machine Learning Research. 2006. Vol. 7. Pp. 1–30.

4. Dietterich, T. G., Lathrop, R. H., Lozano-Pérez, T. Solving the multiple instanceproblem with axis-parallel rectangles // Artificial Intelligence. 1997. Vol. 89. Pp. 31–71.

5. García S., Herrera F. An Extension on «Statistical Comparisons of Classifiers over Multiple Data Sets» for all Pairwise Comparisons // Journal of Machine Learning Research. 2008. Vol. 9. Pp. 2677–2694.

6. Melki G., Cano A., & Ventura S. MIRSVM: Multi-instance support vector machine with bag representatives // Pattern Recognition. 2018. Vol. 79. Pp. 228–241.

7. Peng X., Wang L., Wang X., Qiao Y. Bag of visual words and fusion methods for action recognition: Comprehensive study and good practice // Computer Vision and Image Understanding. 2016. Vol. 150. Pp. 109–125.

8. Quintero-Domínguez L.A., Morell C., Ventura S. WordificationMI: multirelational data mining through multiple-instance propositionalization // Progress in Artificial Intelligence. 2019. Vol. 8. Pp. 375–387.

9. Quintero-Domínguez L.A., Morell C., Ventura S. A propositionalization method of multi-relational data based on Grammar-Guided Genetic Programming // Expert Systems with Applications. 2021. Vol. 168. Art. 114263.

10. Sánchez Tarragó D., Cornelis C., Bello R., Herrera, F. A multi-instance learning wrapper based on the Rocchio classifier for web index recommendation // Knowledge-Based Systems. 2014. Vol. 59. Pp. 173–181.

11. Zafra A., Ventura, S. Multi-instance genetic programming for predicting student performance in web based educational environments // Applied Soft Computing. 2012. Vol. 12. Pp. 2693–2706.

Dilixiati Duolikun,
Master's student,
Belarusian State University

DIGITAL TECHNOLOGY IN CHINA'S JUSTICE

Abstract. The pandemic in 2020 gave a powerful impetus to the development of digital technologies and the maximum digitalization of all spheres of public life. This continued the trend of growing popularity of online education, e-commerce, online communication, including hosting forums, summits, conferences, meetings, brainstorming sessions storms, digital online meetings. Some researchers believe that the global pandemic has been the catalyst of the new, nascent phenomenon of digital globalization. The court system is not an exemption. This article recognizes the China approach of digitalizing justice.

Keywords: artificial intelligence, digitalization; online courts, transparency, legal proceedings, online auctions, cybersecurity, e-filling, QR code-filling

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ПРАВОСУДИИ КИТАЯ

Аннотация. Пандемия, охватившая мир в 2020 г., послужила мощным импульсом цифровизации всех сфер общественной жизни. Возросла популярность онлайн-образования, электронной коммерции, онлайн-общения, включая проведение форумов, саммитов, конференций, совещаний, мозговых штурмов и заседаний в цифровом (онлайн) формате. Некоторые исследователи полагают, что именно пандемия стала катализатором нового зарождающего явления – цифровой глобализации. Цифровая сфера не имеет государственных границ, территориальной принадлежности, не всегда охватывается национальной юрисдикцией государств. Мир становится свидетелем прихода новой культуры – электронной. Судебная система не является исключением. В этой статье рассматривается опыт Китая в цифровизации системы правосудия.

Ключевые слова: искусственный интеллект, цифровизация, онлайн-суды, транспарентность, судебное разбирательство, онлайн-аукционы, кибербезопасность, электронное заполнение, QR-заполнение

Introduction. The rule by law is the fundamental method for administering the country and managing governmental affairs, while justice is a key cornerstone of the system of rule by law. We believe, nowadays the information and communication development index predetermine the leading positions of the "super-powers" in the world arena, as well as some individual domestic social institutions.

In recent years, in order to improve the quality of life of the population and the development of the economy, the introduction of digital technologies in various public spheres is carried out by each State in its own vector and at its own pace. The digital divide between individual States exposes the world community to the global problem of the digital divide between States. In the leading countries of «Industry 4.0» it is difficult to imagine any branch of production or social industry, in which some digital elements are not introduced.

Digital technologies have been integrated into the legal institutions of pioneer states for several decades, the rest of the states, in order to keep up with the general mainstream, actively study their advanced ideas, developments and experience. Already today, China has achieved remarkable successes in digitizing its economy, production, social institutions and law. The unique experience of digitalization of the law and legal institutions of the People's Republic of China represents one of the most topical research topics.

Since 2013, China has been implementing an ambitious strategy for the rule of law in cyberspace. This period the courts began to implement socially oriented development ideas, expressed in the implementation of the strategy of China becoming an Internet power, the state strategy of big data, the program "Internet+, by searching for new opportunities, methods, forms of in-depth integration of modern Internet technologies into the judicial process, the preliminary creation of a framework diversified system of dispute resolution and the implementation of court procedures online, the gradual improvement of the rules of online litigation, Streamlining and increasing the transparency of domestic cyberspace, effectively promoting the modernization of State administration systems.

Internet court is a major institutional innovation whereby China's courts actively address the judicial needs in the Internet era and implement the Internet power strategy: in August 2017 – September, 2018 Hangzhou Internet Court, Beijing Internet Court, and Guangzhou Internet Court were successively established [1. P. 89].

In September 2018, the Supreme People's Court issued judicial interpretations of trials before Internet courts, clarifying the jurisdiction, appeal mechanism, online litigation rules, and requirements for construction of litigation platform of Internet Courts [1, p. 89]. Internet Courts have actively promoted the "online resolution of online disputes", facilitated the online verification of litigant's identity, online collection of evidentiary materials, etc., thus significantly improving judicial efficiency.

In Hangzhou Internet Court, the online case-filing rate has reached 91.2%, the online court-session rate has reached 61.9%, the online case-concluding rate has reached 83.6%, the online trial period has averaged 41 days, saving 60% if compared with the traditional trial mode [1. Pp. 89–90]. The Internet Courts have successfully and efficiently adjudicated a number of difficult and complicated Internet-related cases of new types, including the ownership of big data, the liability for contracting fault in online shopping, and the ownership of copyright in artificial intelligence works, thus strongly promoting the rule of law in cyberspace governance [1. Pp. 89–90].

I. Legislation of digitization of justice

There are several new legal acts came into force after 2013 in China. Here is a list of the main ones [9–16]:

The supreme people's court on the people's court trial audio and video recording of a number of provisions of the law release [2017] No. 5, release date 2017-02-22 implementation date 2017-03-01).

The Supreme People's Court "Several Opinions on Further Strengthening the Work of Civil Service" Fa Fa [2017] No. 19, Release Date July 19, 2017.

Supreme People's Court Notice on Further Accelerating the Work of Simultaneous Generation and In-depth Application of Electronic Dossiers Fa [2018] No. 21, January 16, 2018.

The Pilot Program for Reform of the Complexity and Simplicity of Civil Litigation Procedures issued by the Supreme People's Court, Law [2020] No. 10.

The Supreme People's Court formulated the Implementation Measures for the Pilot Reform of the Complexity and Simplicity of Civil Litigation Procedures, Law [2020] No. 11.

II. Digitization of legal proceedings

The convergence of digital technologies has led to profound changes in the way Chinese courts conduct litigation. The digitization of legal documents, case management systems, and online case filing platforms has streamlined processes and reduced paperwork and manual errors. For example, since May 2015, the people's courts have introduced the case filing registration system and eliminated the prior examination. The e-filing system speeds up the filing and processing of cases, increasing efficiency and reducing administrative burdens. As of 2021, the courts filed over 64.89 million cases, with an on-the-spot case registration rate of over 95%.

The Chinese courts have been forming a new pattern of case filing with on-the-spot case filing as main method, with online case filing, self-service case filing, crossregional case filing, collaborative case filing and so forth as supplementary methods. To file a lawsuit is more conveniently and quicker, the efficiency of case filing has improved significantly.

As of the end of 2021, 3,044 courts nationwide had introduced online case filing service, and 2.38 million cases had been filed online; 1,155 courts had provided cross-regional case filing service, and 120,000 cases had been filed via the cross-regional filing systems; 1,863 courts had set up self-service case filing areas, and litigants or lawyers had filed 1.03 million cases by themselves [2]. Few courts in Beijing, Tianjin and Hebei have established a new mode of collaborative case filing mechanism: litigants' equal access to the inclusive, convenient and efficient case filing services provided irrespective of whereabouts. The People's Court of Pudong New Area, Shanghai has developed a "QR code" self-service case filing system, it takes 15 minutes to filed the case [1. P. 107].

Thus, China has built a trial support system and a data-sharing and exchange system based on big data intelligent services, improved the judicial trial information resource base, and widely applied big data analysis systems in courts at all levels.

First, a judicial trial information resource base covering core data has been fully completed. The judicial trial information resource base includes trial execution information, judicial personnel information, informationization management information, judicial

research and judicial government information. The above information constitutes the framework of judicial big data, through which it is possible to have a glimpse of the number of cases, the ratio of cases received and closed, the rate of execution in place, the ratio of persons to cases, and other key elements, thus providing practical data support for judging judicial efficiency, evaluating judicial justice, and allocating judicial resources.

Second, a nationwide data quality management system has been formed. People's court data statistics have gone through three stages: manual card statistics, computerized statistics and information system statistics. With the in-depth construction of court informatization and the establishment of data quality management system, the Supreme People's Court has formed a nationwide big data management and service platform, and the Higher People's Courts have set up judicial data quality control mechanisms or data governance and control application systems. With the support of the platform and system, the confidence level of structured data on cases in courts at all levels has remained stable at over 99% for a long period of time [2].

Third, the two-tier data sharing and exchange system covering the whole country is functioning substantially. Data exchange and sharing is conducive to improving the quality and efficiency of data utilization and maximizing the dividends of informatization construction. Within the courts, the Supreme People's Court and the Higher People's Courts have established a data sharing and exchange platform to guarantee the unimpeded flow of information and data within the courts; the courts above the high level have increased their capacity to support the exchange of information on classified networks to safeguard the security of judicial data and networks; and the intermediate and basic-level courts have strengthened the capacity of sharing and exchanging data among the courts to enable the courts to realize data sharing at the cross-tier, cross-network, cross-regional, and cross-application levels. data sharing across levels, network systems, regions and applications.

III. Better access to legal information

Digital technology has paved the way for better access to legal information and resources for both legal professionals and the public. Online databases and legal research platforms have become indispensable tools for lawyers, judges and academics to help them learn about the latest case law. In addition, legal information that used to be found only in law libraries is now readily available to the public, thus contributing to legal literacy and enabling citizens to understand their rights and obligations.

The so-called "Four Main Platforms of Open Trial of the National Courts of the People's Republic of China" have been successively established, namely:

1. China Judicial Process Information Online [5], officially launched from 13.11.2014. As of October 31, 2022, the Judicial Disclosure Network in China had more than 24 million registered cases, more than 1.1 billion units of open case files.

2. China Judgements Online [6], from January 2014. As of April 30, 2020, the total number of court documents published exceeded 91.8 million units, and attendance exceeded 43.8 billion clicks.

3. Open Court Hearing Network of China [7], from September 2016. As of April 30, 2020, more than 6.9 million court cases have been broadcast online through this network, and the number of page visits exceeded 23.6 billion clicks.

4. The Executive Production Disclosure Network of China [8] from June 2018. More than 22.7 million documents have now been published through it.

The good sample of success digitalization in justice is online auctions. In order to overcome the shortcomings of conventional auction methods, the Supreme People's Court, absorbing and distilling the experiences of online judicial auctions in lower courts, has established a new judicial auction mode that online auctions are general and traditional auctions are exceptional, and promulgated judicial interpretations regarding online judicial auctions, requiring full promotion of online judicial auctions nationwide and improvement of related supporting systems from January 1, 2017. Up to now, 92.5% of the courts nationwide (namely 3,260 courts) have fully adopted online auctions, and over 80% of the judicial auctions have been conducted online. Owing to the implementation of online judicial auctions, the successful auction rate and premium rate have increased exponentially, and the rate of failed auction and price reduction as well as the auction costs has dropped significantly. Online actions effectively eliminate the rent-seeking probabilities, cut off the illegal interest chain, and bring about "zero complaint" about violation of laws and disciplines during auctions [1. P. 123; 2].

Just in the beginning of reform in March 2017 to December 2018, the courts nationwide have conducted over 940,000 online auctions and thereby sold over 270,000 items for RMB 604.9 billion, with successful auction rate of 70.8% and premium rate of 64.3% and saving commissions of RMB 18.6 billion for litigants [1. P. 123]. To tackle the low efficiency of appraisal during judicial auctions, courts nationwide have diversified methods of appraisal such as bargaining between litigants, targeted inquiries, online inquiries and entrusted appraisals, and have established a unified online appraisal platform. With appraisals becoming more standardized and informatized, the efficiency of property disposal has been improved and the burden on litigants has been alleviated.

IV. Enhancing justice transparency

Transparency in the justice system is essential to maintaining the rule of law and public trust.

"Transparent" means that the public would have online access not only to the documents in court files, but also to the answers to millions of the most important questions regarding the system's performance [4].

In addition to the above-mentioned, Internet services on judicial disclosure, the courts of the People's Republic of China are increasingly increasing the scope of their presence in popular social networks. For example, as of October 31, 2019, in the social network Sina Weibo (the Chinese analogue of Facebook) 3 585 accounts were registered to the courts of the People's Republic of China of various levels, the total number of subscribers exceeded 81.3 million. network users. The most active and popular of these accounts is the account of the Supreme People's Court of the People's Republic of China, through which 23,372 publications were posted as of 30 April 2020, the number of subscribers is more than 17.7 million network users. More than 14,000 publications have been made on the public WeChat account of the Supreme People's Court of China, the number of followers has exceeded 1.51 million [2].

Digital technology has played a key role in increasing the transparency of China's judicial system. The live streaming of court hearings, which is widely promoted, allows the public to watch court proceedings remotely, thus ensuring accountability and reducing opportunities for corruption.

V. Artificial Intelligence in the Justice System

Artificial intelligence (AI) has become a revolutionary force in China's justice system. Smart contracts, AI assistants, e-reviews, legal AI, lawyers and data synthesis - these new technologies help lawyers make informed decisions. For example, the "Hi-Law" team from East China University of Political Science and Law has developed a project called "Ai Lawyer", which is an intelligent service system. The intelligent service system "Ai Lawyer", developed by the team of "Hi-Law" of East China University of Political Science and Law, can accurately analyze legal relationship problems and identify litigation cases through the comprehensive application of large language model and knowledge map, and give corresponding legal advice [17]. Although the use cases of AI in the legal industry are not yet popular enough, the end is predictable and is likely to push the envelope. It is foreseeable that the application of AI in the legal industry will become more well-established in the future, helping lawyers to provide high-quality services and better serve the society.

VI. Challenges and Concerns

Despite the many benefits of digital technology, its integration into China's justice system is not without challenges. One important issue is the digital divide, which can make access to justice difficult for marginalized members of society who lack Internet connectivity or digital literacy. To avoid reinforcing the existing divide, it is important to ensure inclusiveness.

Cybersecurity is another key issue. As the justice system becomes increasingly dependent on digital infrastructure, protecting sensitive legal information from cyber threats becomes even more important. Ensuring the confidentiality and integrity of digital records is critical to maintaining public trust.

Conclusion. In the information age, the judicial needs of citizens and companies are becoming increasingly diverse. The new Chinese judicial system is designed to address the challenges of making trials even more accessible, convenient, more efficient, more accurate, more transparent in the country, and to reduce litigation costs.

The use of digital technologies in China's judicial system has brought profound changes that affect the conduct of court proceedings, access to legal information, and the provision of transparency. Therefore, enhancing justice data sharing and exchange, realizing information and resource sharing, and promoting the intelligent development of justice and global justice cooperation will surely become the future development trend in the field of justice.

The People's Republic of China's Internet Court Procedure is a crystallization of modern technical achievements of mankind and the judicial and law enforcement practice of the justice agencies, it certainly goes with the times and will be further improved in accordance with the development of society, meeting the needs of the state, society and individual digital era.

References

1. Chinese Court Judicial Reform (2013–2018). The White Paper on judicial reform of Chinese court from 2013 to 2018 was issued by the Supreme People's Court (SPC) at a press conference on Feb 27. URL: http://www.chinadaily.com.cn/specials/ChineseCourtJudicialReform2013-2018.pdf

2. LoPucki, Lynn M. The future of court system transparency. Confidentiality, Transparency, and the U.S. Civil Justice System. URL: https://doi.org/10.1093/acprof:oso/9780199914333.003.0009

3. China Judicial Process Information Online. URL: https://splcgk.court.gov.cn/gzfwww/.

4. China Judgement Online. URL: http://wenshu.court.gov.cn

5. Open Court Hearing Network of China. URL: http://tingshen.court.gov.cn

6. Provisions of the Supreme People's Court on Several Issues Concerning the Trial of Cases in Internet Courts Fa, 2018.

7. Supreme People's Court of the People's Republic of China. URL: https://english.court.gov.cn/2015-07/16/c_769578.htm

8. Shestakova I. G. New temporality of digital civilization: the future has already come. Nauchno-tekhnicheskie vedomosti SPbGPU. Gumanitarnye i obshchestvennye nauki. 2019. № 10(2). Pp. 20–29.

9. Supreme People's Court Notice on Further Accelerating the Work of Simultaneous Generation and In-depth Application of Electronic Dossiers Fa [2018] No. 21, January 16, 2018.

10. The Executive Production Disclosure Network of China. URL: http://zxgk.court.gov.cn.

11. The supreme people's court on the people's court trial audio and video recording of a number of provisions of the law release [2017] No. 5, release date, 2017.

12. The Supreme People's Court "Several Opinions on Further Strengthening the Work of Civil Service" Fa [2017] No. 19, Release Date, 2017.

13. The Decision of the Standing Committee of the National People's Congress on Authorizing the Supreme People's Court to Carry Out a Pilot Reform of the Complexity and Simplicity of Civil Litigation Procedures in Some Areas, 2019.

14. The Pilot Program for Reform of the Complexity and Simplicity of Civil Litigation Procedures issued by the Supreme People's Court, Law [2020] No. 10.

15. The Supreme People's Court formulated the Implementation Measures for the Pilot Reform of the Complexity and Simplicity of Civil Litigation Procedures, Law [2020] No. 11.

16. The Supreme People's Court's Notice on Strengthening and Standardizing Online Litigation During the Prevention and Control of the New Crown Pneumonia Epidemic.

17. The Huazheng students participate in the creation of "AI lawyers" The project was selected as a typical case database of China Science and Technology Law Society. URL: https://mp.weixin.qq.com

E. E. Gulyaeva,
PhD in Law, associate professor,
Diplomatic Academy of the Ministry of Foreign Affairs of Russia

CONTEMPORARY LEGAL ISSUES ON NEW TECHNOLOGIES

Abstract. This article reviews the contemporary legal issues on new technologies. The object of the study is public relations regulated by both international and national law, which include certain actions for the provision of using digital technologies in diplomacy, artificial intelligence in diplomatic service, creating medical data base. In the midst of the ongoing technological revolution, the discussion surrounding the necessity of preserving personal data gains eminence in the field of studying the human genome within the digital realm. This discourse also highlights the crucial goal of preventing any backward movement towards eugenic practices and emphasizes the obligatory adherence to ethical and legal frameworks by sovereign entities.

Keywords: communication, digital data, artificial intelligence in diplomacy, cybersecurity, international law, technological revolution

СОВРЕМЕННЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ НОВЫХ ТЕХНОЛОГИЙ

Аннотация. В статье рассматриваются современные правовые вопросы, касающиеся новых технологий. Объектом исследования являются общественные отношения, регулируемые как международным, так и национальным правом, в сфере применения цифровых технологий в дипломатии, искусственного интеллекта на дипломатической службе, созданию базы медицинских данных. В условиях продолжающейся технологической революции дискуссия о необходимости сохранения персональных данных приобретает особую значимость в области изучения генома человека в цифровом пространстве. В этом дискурсе также выделяется важнейшая задача предотвращения любого движения назад к евгеническим практикам и подчеркивается обязательное соблюдение этических и правовых рамок суверенными субъектами.

Ключевые слова: коммуникация, цифровые данные, искусственный интеллект в дипломатии, кибербезопасность, международное право, технологическая революция

> We need international and national policies and regulatory frameworks to ensure that these emerging technologies benefit humanity as a whole. We need a human-centered AI. AI must be for the greater interest of the people, not the other way around, – UNESCO, 2021.

Introduction. In 2021, the Russian scientific community broadened the spectrum of academic disciplines by including four additional clusters in its catalogue of scientific specializations. These are computer science and informatics, biotechnology, subsurface use and mining sciences as well as cognitive sciences. This proves that the issues of this type are especially significant for the foreign and domestic policies of the Russian Federation. Legitimate regime for using new technologies in a digital era was adopted through the legal instruments.

So, in 2020, to the Article 71 of the Constitution of Russia have been made the amendments to paragraphs «d», «e», «i», «m», «r», «t», especially concerning the use of new technologies in internal and external policy, to such adjustments were added the following areas: i) federal energy infrastructure, atomic energy, and fissionable materials; statewide mobility networks, telecommunications, data, ICT, media and communication industry; outer space endeavors; l) defense and security; military-industrial complex; establishment of protocols for the trade and acquisition of weaponry, ammunition, military machinery, and related military assets; synthesis of toxic agents and narcotics as well as regulations governing their use; assurance of individual, societal, and state security while employing information technologies and the flow of digital data.

To illustrate it, on March 31, 2023, The Concept of the Foreign Policy of the Russian Federation approved by Decree of the President of the Russian Federation No. 229, in para. 7 «Humanity is currently going through revolutionary changes… Structural transformation of the world economy, its transfer to a new technological basis (including the introduction of artificial intelligence technologies, the latest information and communication, energy, biological technologies and nanotechnologies), the growth of national consciousness, cultural and civilizational diversity and other objective factors accelerate the process of shifting the development potential to new centers of economic growth and geopolitical influence and promote the democratization of international relations». Moreover, para. 9 stated that «Serious pressure is being put on the UN and other multilateral institutions the intended purpose of which, as platforms for harmonizing the interests of the leading powers, is artificially devalued. The international legal system is put to the test: a small group of states is trying to replace it with the concept of a rules-based world order (imposition of rules, standards and norms that have been developed without equitable participation of all interested states). It becomes more difficult to develop collective responses to transnational challenges and threats, such as the illicit arms trade, proliferation of weapons of mass destruction and their means of delivery, dangerous pathogens and infectious diseases, the use of information and communication technologies for illicit purposes, international terrorism, illicit trafficking in narcotic drugs, psychotropic substances and their precursors, transnational organized crime and corruption, natural and man-made disasters, illegal migration, environmental degradation. The culture of dialogue in international affairs is degrading, and the effectiveness of diplomacy as a means of peaceful dispute settlement is decreasing. There is an acute lack of trust and predictability in international affairs.

As mentioned in para 26. of the Concept "If foreign nations or their affiliations engage in hostile actions that pose a threat to sovereignty and territorial integrity of the Russian Federation, including those involving restrictive measures (sanctions) of a political or economic nature or the use of modern information and communication technologies, the Russian Federation considers it lawful to take the symmetrical and asymmetrical measures necessary to suppress such unfriendly acts and also to prevent them from recurring in future".

In addition, it is noted in para. 30 that "…In order to ensure international information security, counter threats against it, and strengthen Russian sovereignty in the global cyberspace, the Russian Federation intends to give priority attention to:

1) strengthening and improving the international legal regime for preventing and resolving interstate conflicts and regulating activities in the global cyberspace;

2) shaping and improving an international legal framework for countering criminal uses of information and communication technologies;

3) ensuring the safe and stable Internet operation and development based on the equitable participation of states in the management of this network and precluding foreign control over its national segments;

4) adopting political, diplomatic and other measures aimed at countering the policy of unfriendly states to weaponize the global cyberspace, use information and communication technologies to interfere with the internal affairs of states for military purposes, as well as limit the access of other states to advanced information and communication technologies and increase their technological dependence…".

The contemporary doctrine of Russian foreign policy as well included to traditional methods of diplomacy the "soft power", which become an integral part of efforts to achieve foreign policy objectives. This primarily involved the tools offered by civil society, as well as various methods and technologies – from information and communication, to humanitarian and other types.

Cybersecurity in International Law

On November 2021 at the plenary meeting of the First Committee of the 76th session of the UN General Assembly [13] on agenda item, "Developments in the field of information and telecommunications in the context of international security" by consensus adopted a Russian-American resolution on the responsible behavior of states in cyberspace. The fact that Russia and the United States for the first time submitted such a document to the General Assembly for consideration. This is a historic decision and adopting a draft UNGA resolution consolidates the reestablished atmosphere of consensus in the global discussion on international information security under the UN auspices. The draft resolution lays a strategic basis for continuing the negotiation process: it expresses support for the OEWG on security of and in the use of ICTs 2021-2025 and reaffirms its mandate, as set forth in UNGA resolution 75/240. The document also reflects such indisputable principles of ensuring international information security as promoting peaceful use of ICTs, preventing their use for criminal and terrorist purposes, and preventing conflicts in information space. The possibility of developing additional rules, norms and principles of responsible behavior of States, including additional binding obligations, was confirmed. At the time of the adoption of the resolution, at least 105 states decided to become its co-sponsors, which speaks of broad support for the Russian-American initiative. Previously, Moscow and Washington promoted two competing cybersecurity negotiating mechanisms at the UN. We believe that the adoption of the Russia-US draft resolution will become a meaningful contribution to strengthening international peace and security in the use of ICTs.

In 2021 at least 60,000 organizations around the world have been compromised due to vulnerabilities in Microsoft software. The author of the publication pointed out that if the growth in the number of victims of the cyber attack continues, the incident can be equated with a global cyber security crisis.

On July 2021, Russia has come up with a proposal to the United Nations (UN) to classify cybercrime into 23 types, and not nine, as is the practice at the moment. The project reflects 23 corpus delicti, including unauthorized access to personal data, illegal distribution of counterfeit medicines and medical products, terrorism, extremism, rehabilitation of Nazism, illegal drug trafficking, weapons, involvement of minors in illegal activities and much more.

In the contemporary milieu, there has been a substantial escalation in the frequency of cybercrimes. New strains of malicious software employed for unlawful objectives emerge in a consistent manner. As per the assessments of specialists, the financial detriment inflicted upon the global economy due to transgressions perpetrated through information and communication technologies reaches into the trillions of US dollars. The magnitude of this issue necessitates efficacious mechanisms for the legal delineation of interactions within the cyberspace domain. Cybersecurity stands as a preeminent theme within contemporary international law, bearing immense significance for the assurance of national security for sovereign entities. Information and communication technologies wield the potential to exert adverse influences upon economic, social, cultural, and political affiliations, thereby undermining the economic and defensive capacities of both the state and society. In this context, the global community displays a profound vested interest in the establishment of a comprehensive multilateral legal framework to facilitate collaboration within the realm of cybersecurity. However, a cohesive approach to resolving this matter at the international level remains elusive. The complexity of legal governance in the realm of cyberspace is particularly intricate due to its virtual and interface-based nature.

Consequently, while the established principles and regulations of extant international law are applicable to the digital sphere, there exists a pressing need to harmonize the prevailing international legal framework governing cyberspace. This harmonization should encompass the unique features of cyberspace and be directed towards the efficacious counteraction of illegitimate use of Information and Communication Technologies (ICT).

Currently, states predominantly concentrate on a limited spectrum of issues encompassing human rights and data privacy, among others. The inclination to establish an effective cooperative mechanism is not uniformly shared among all states. A number of states exhibit resistance to the formulation of novel international legal instruments, thereby underscoring the existing complexities in this arena. Subsequently, the initiative set forth by the Russian administration with regard to the United Nations Convention on Collaborative Measures Against Informational Offenses has not garnered concurrence. This circumstance has precipitated the dearth of an all-encompassing, globally applicable jurisprudential architecture for intergovernmental cooperation in the domain of the virtual realm.

The comprehensive scrutiny undertaken has revealed that, notwithstanding the adaptability of prevailing international legal precepts to the realm of informational activities, the imperative of a universalized international legal regimen for the governance of cyberspace emerges, contingent upon the inherent attributes thereof. The underlying intent is to efficaciously counteract the illicit deployment of information and commu-

nication technologies. Noteworthy efforts of sovereign entities to codify specialized protocols of engagement in the digital realm currently remain confined to a restricted ambit encompassing issues pertaining to human rights, data protection, and the like. Not all nation-states exhibit a vested interest in the establishment of a modernized and efficacious framework to facilitate cooperative endeavors within cyberspace. A number of such entities are overtly adversarial to the conception of novel international legal instruments. This very contention accounts for the disapprobation faced by the Russian endeavor aimed at the adoption of the United Nations Convention on Collaborative Measures Against Informational Offenses. In consequence, the resultant void precipitates the inadequacy of a comprehensive, universalized international legal infrastructure tailored to galvanize harmonious collaboration within the domain of cyberspace. The synthesis of scholarly discourse and empirical instances propels the author to assert that a critical exigency materializes for the establishment of a comprehensive, universalized international legal framework that nurtures cooperative mechanisms within the ambit of cyberspace.

Digital intelligence in the diplomatic corps

Professionals are contemplating the pragmatic utilization of AI amid the landscape of global diplomacy. According to their reports, in 45 years artificial intelligence will be better than people to cope with all types of work; moreover, is quite applicable in the diplomatic service. So, according to American scientists, by 2024 AI will be better at handling translations, by 2026 it will be able to write essays on given topics better than high school students, by 2027 it will completely replace people driving trucks, by 2049 it will easily write bestsellers, and by 2053, it is better to operate a human surgeon. For instance, a certain amount of automation with the help of AI will not interfere with diplomatic work, and not only at the level of consulates and paperwork, but also at the level of international negotiations and public diplomacy. AI could help improve communication between governments and citizens of different countries by removing language barriers, improve the security of diplomatic missions using image recognition and information sorting technologies, support international peacekeeping operations and prevent disruptions when providing financial assistance to other countries.

Let consider us the simplest level of use of AI in diplomacy. The AI system enters into this business: using the method of evaluative and descriptive analytics, it studies the data of the work of the consulate in the last half-decade, reveals hidden patterns and predicts that next year the peak demand for passports, visas and certificates is most likely in August, May and December. The next year is approaching, and the AI forecast for May and August is confirmed, and with December, for example, it was wrong. Then the updated data is entered into the AI system, and considering this, it issues a new, more accurate forecast for the next year. Anticipated outcomes suggest an amplified operational efficiency within a specific consulate. Subsequently, this approach could be extended to assist other consulates grappling with analogous challenges.

With the development of quantum computing technologies, AI may very soon become an important tool, for example, in resolving diplomatic crises. "AI systems will be able to help embassies and foreign ministries to comprehend the essence and scale of events in real time, simplify the decision-making process, deal with public expectations

and help end the crisis," writes Corneliu Bjola. Now the integration of AI into this work is possible only under human control. As far as negotiation is concerned, AI cannot yet replace a human in the conduct of this process or in decision-making. On the other hand, it can help find the best negotiation strategy by timely and quickly selecting the necessary information, analyzing the data obtained and making predictions, which could take days or even weeks for a person.

Current issues of legal regulation of genomic information at the universal and regional levels

Amidst the backdrop of the ongoing technological revolution, it becomes imperative to delve into the significance of safeguarding personal data within the realm of biotechnological endeavors in the digital domain [3. Pp. 44–53].The realms of biological and medical research, coupled with technological advancements, have ushered in remarkable strides in healthcare. However, these commendable advancements concurrently engender ethical dilemmas that bear ramifications for individuals and the preservation of their rights and dignity [2. Pp. 16–37].

The "Fourth Industrial Revolution" [8. P. 320] has brought to life innovative technological solutions in the biological [6. Pp. 56–60; 10. Pp. 36–40; 11. Pp. 144–154], physical, and digital blocks, which are prompting states to deploy more active programs to support the digital transformation that is objectively occurring throughout the world. Today, the most important elements of social life have already been moved into a virtual space with the specific temporality of new technologies, which has led to revolutionary transformations also in the system of governance (from e-government and smart cities to the Internet of Things). "This prompts the application of political incentive mechanisms (universal digitalization programs, etc.)" in the context of the emerging digital civilization [9. P. 26].

In particular, in the view of the authors, the Russian Federation has a legal instrument defining the term "confidential data related to the activities of a legal entity" Decree of the President of the Russian Federation "On approval of the list of information of confidential nature" № 188 March 6, 1997 which specifies the list of confidential information.

In addition to outlining the facts and private events of a citizen allowing personal identification, the list includes confidential information and "information related to business activities", "service data", "information about the essence of invention, utility or industrial model prior to the official release" and "vocational-related data".

In 2021, the EU European Commission approved the European Strategy for Data, which focuses on putting people first in the development of technology, as well as to contribute to the security and fostering of European values and rights in the digital world according to the EU Charter of Fundamental Rights 2000.

In the approved document for Data Management in Europe, the "Health data" category is specified in a separate paragraph, which aims at: improving personalized treatments, facilitating improved health services and better medical and medication-related assistance for rare or chronic diseases, which will save about 120 billion euros per year in the EU health sector and to ensure a more effective and rapid response to the global health crisis caused by COVID-19. The Commission also endorsed the proposal

of Member States to adopt the Pact on research and innovation in Europe the gist of which is to become a solid basis within the EU for the new European Research Area (ERA). A potential international treaty will be based on general principles of research and innovation in Europe, including such values as freedom of scientific research, equal opportunities for all, free popularization of research and knowledge, inclusiveness and social responsibility.

The EU market of genomic research is developing on a large scale and very rapidly. Genetic technologies are being improved and successfully implemented. That is why there is an urgent issue of enhancing legal protection and legal guarantees of confidentiality down to the safeguards of human genomic data in EU criminal law.

In the EU, among the three pillars of Horizon Europe, which is the funding program for research and innovation, one pillar is devoted to global challenges and European industrial competitiveness. The cluster Health in this pillar stresses the need to develop health technologies, mitigate health risks, protect populations as well as promote good health and well-being of citizens. There are high expectations for genomic research, which has been one of the most dynamic sectors in recent decades.

Currently, the EU countries are implementing projects aimed at collecting, researching, storing, and transmitting human genetic information with the subsequent application of the acquired data in everyday life. All new technologies and developments in the field of the human genome have been widely introduced among such areas as medicine, pharmaceuticals, industrial biotechnologies, agriculture, and forensics. With the development of omics sciences, e.g. genomics, large arrays of complex data (Big Data) have been accumulated. This leads to a closer interaction of legal protection mechanisms with bioinformatics and biostatistics.

The utilization of genomic sequencing technology is experiencing ongoing expansion across various domains, encompassing applications as diverse as crime detection and disease causality identification. Pertaining to the latter, there has been a mounting fascination with the adoption of CRISPR-Cas9 DNA editing methodologies, facilitating meticulous DNA manipulation through specialized protein-mediated precise cleavage and recombination.

As genomic technologies and genetic engineering advance, European Union nations are actively exploring novel avenues and strategies to guarantee the biosafety of individuals and society at large. Within the European community, a growing consciousness is emerging regarding the imperative to adeptly safeguard constitutional and civil human rights amidst the unfolding panorama of scientific exploration and its consequential implementation.

There is a vital requirement to formulate efficacious ethical and legal strategies for addressing challenges stemming from the integration of genetic-data-driven personalized medical technologies within healthcare practices. Equally crucial is the adherence to the bioethical principle of justice, in conjunction with the traditional "non-maleficence" principle, as an excessive comprehension of an individual's genome can carry potential harm [5].

In 1991, the European Group on Ethics in Science and New Technologies (EGE) within the European Commission was established. Currently, it is working on the issues

of human genome editing, the use of artificial intelligence, and potential challenges to humanity.

European Commission European Group on Ethics in Science and New Technologies – EGE has been established within the EU European Commission. This EU institution is currently working on the topics of Human Genome Editing, Artificial Intelligence and future potential challenges to humanity. Accordingly, in May 2021, the Group submitted a document containing **"design for values", "value-sensitive design", "ethics by design"** in the context of policy and regulation of the principle of "confidentiality" in data protection and "transparency and fairness" in AI management. As for the experts' input such an approach should be an integral part of European, education, production, monitoring and management of innovation and new technologies. Moreover, in the recent official statement "Values for the future: the role of ethics in European and global governance" importance attached to the role of values and experts emphasized the central and active role of ethics in in European and world administration. Very important for legal regulation in the EU is the WHO instrument called "Proposed International Guidelines on Ethical Issues in Medical Genetics and Genetic Services".

Some experts incorporate somatic rights, genetic rights, the right to access personal data, the right to be forgotten, the right not to know and not to be informed, the right to correct and clarify personal data, etc. in the fourth-generation human rights. New achievements of the fourth industrial revolution in the field of medicine and genetic engineering provide many advantages aimed at protecting human health (ZFN, CRISPR, Antisense, TALEN, etc.). However, questions arise concerning the personal rights of each citizen, public health [7], and the principles of humanity and genetic privacy [1. P. 1; 6].

The Council of Europe Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine: Convention on Human Rights and Biomedicine (ETS No. 164) was adopted by the participating States in Oviedo (Spain) on 4 April 1996, and enforced on 1 December 1999. Under the Convention, it is important to obtain and secure the person's consent for medical intervention and donorship as well as transplantation of human cells, tissues, organs, genetic studies of the brain, and the use of information technologies in this area, including in the processing of Big Data.

This Convention is the only international legally binding instrument on the protection of human rights in the biomedical and genomic field. It is aimed at ensuring respect for human rights in the context of the technological revolution and securing the rights of patients by creating their updated code.

As of the present day, the Convention in question has undergone complete ratification by merely 17 member states of the European Union. These include Greece, Slovenia, and Slovakia in 1998; Spain and Denmark in 1999; Portugal, Romania, and the Czech Republic in 2001; Hungary, Cyprus, Lithuania, and Estonia in 2002; Bulgaria and Croatia in 2003; Finland in 2009; Latvia in 2010; and France in 2011. Nevertheless, it is noteworthy that 5 member states, namely Austria, Belgium, Germany, Ireland, and Malta, have refrained from signing the Convention. Additionally, there are 5 states that have appended their signatures but have not yet ratified it–these are Italy, Luxembourg,

the Netherlands, and Sweden, all in 1997, and Poland in 1999.In the EU, the doctrinal regulation of the genetic information flow is done either by various instruments adopted by the UN agencies like WHO, UNESCO, etc. or by professional healthcare and bioethics organizations like the World Medical Association, the Council for International Organizations of Medical Sciences, the European Group on Ethics in Science and New Technologies, the European Bioinformatics Community, the European Bioinformatics Institute (EMBL-EBI), the European Society of Human Genetics, the European Society of Human Reproduction and Embryology, etc.

In the context of the fourth technological revolution, there is a need to discuss the importance of personal data protection in the field of human genome research in the regional and national jurisdictions of the EU Member States as well as in the European cyberspace [3. P. 386].

The strides made in healthcare owe much to advancements in biological and medical research, as well as innovations in biotechnologies. Yet, these accomplishments have concurrently brought forth ethical quandaries that intersect with the safeguarding of human rights and dignity in areas encompassing genetics, human organ and tissue transplantation, and embryonic interventions. This holds true not only for the establishment of personalized and national biobanks, and the application of contemporary technologies in the construction of health databases, but also for the initiation of discourse regarding the concept of genetic responsibility, sparking deliberations in the legal realm and within the public sphere.

In the European Union, general medical and genetic data is considered personal and confidential. This status was legally fixed in the Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The same meaning of genetic data is stated in UN instruments. In particular, WHO defines it as confidential personal information of a special socio-psychological and medical nature, which is important not only for the patient himself/herself but also for a wide range of his/her relatives.

At the level of the Council of Europe, the relevant provisions of Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms are interpreted by the European Court of Human Rights. The Court has repeatedly acknowledged that the protection of personal data, including medical and genetic information, is crucial to the realization of the right to respect for private and family life. The requirement to respect the confidentiality of health data is a fundamental principle in all legal systems of the Parties to the Convention.

The Council of Europe has established stricter rules for the processing of personal information related to human genes. In particular, the issue is covered in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of January 28, 1981 [13]. The Convention contains requirements for the principles of proportionality, transparency, minimization, and legality of the collection, processing, and storage of personal data as well as privacy by design and data protection during data processing, among other things for national security. Exceptions and restrictions are possible in accordance with the provisions of the Convention under independent control

and supervision. This instrument also introduces a new category of sensitive data. This is genetic data, biometric data, and data on the ethnic origin of a person. Under Article 7 "Data security" of the Convention, appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration, or dissemination. In addition, the Convention introduces the obligation for personal data operators to notify the authorized supervisory authority about data leaks and establishes clear legal procedures for cross-border data flows as well as the obligation for authorities to report data violations.

Article 4 of the Regulation of the European Parliament and of the Council of the European Union 2016/679 of 27 April 2016 On the protection of individuals in the processing of personal data and on the free circulation of such data and on the repeal of Directive 95/46/EC (General Regulation on the Protection of Personal Data)» by "processing" means any transaction or set of transactions involving personal data with or without automated tools such as collecting, recording, organizing, structuring, storing, modifying and changing, retrieving, counselling, use, disclosure by transferring, distribution or otherwise provision, ordering or combining, limitation, erasing or destroying.

The previously enforced Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (Data Retention Directive) was revoked. On 8 April 2014, the Court of Justice of the European Union in its C-293/12 and C-594/12 Judgment declared the Directive invalid. Actually, it was declared void because its provisions contradicted the important principle of European law, which proclaims proportionality of limits on the exercise of fundamental rights [4. P. 27].

The EU pays special attention to the legal regulation of metadata processing as a tool for classifying, organizing, and characterizing data or content (so-called "data about data"). This includes traffic data, location-based data, etc. According to the interstate standard DIN ISO/IEC 17788-2016, "data about data" is classified as "cloud service derived data" managed by the cloud computing service provider and received by the consumer of the cloud computing service through the interaction with the cloud computing service. Cloud service derived data includes an event log with the information about who used the service, at what time, what functions and data types were involved, etc. There is also information about the number of authorized users and their IDs.

When assessing the appropriate protection of personal data of third countries within the European Union Regulation 2016/679, the assessors take into account the country's participation in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as participation in multilateral or regional systems for the protection of personal data and compliance with international obligations. The information is from paragraph 105 of the General Data Protection Regulation (GDPR) Preamble.

Under Articles 28 (3) and 28 (9) of the GDPR, in order to ensure data protection, a contract for the use of a cloud computing service (concluded in writing or electronically) must set out the subject-matter and duration of the processing, the nature and purpose of

the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

Chapter V "Transfer of personal data to third countries or international organizations" of the GDPR defines the procedure for cross-border transfer of personal data outside the European Union. For example, under Article 45 of the GDPR, a cross-border transfer may take place where the Commission has decided that the third country, a territory, or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Moreover, such a transfer does not require any specific authorization.

A number of the EU jurisdictions provide for specific DNA databases used in criminal justice systems. These are usually designed to store DNA profiles for the identification of suspects and convicts in criminal investigations and proceedings.

The European Union and individual Member States are currently introducing criminal law regulations for the protection of personal genetic data from illegal use or forgery, from making changes to the human genome, modifying the progeny genome (the germ line), or the use of potentially harmful somatic gene therapies, in particular, through the use of CRISPR technologies.

Member States are supposed to refer to the Oviedo Convention, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the MEDICRIME Convention, and the Convention on Cybercrime. In addition, there is the European Charter of Patients' Rights (ECPR), which represents the basic rights of patients in the field of health care.

The legal landscape, regarding genomic law, human rights in the field of genetics and assisted reproductive and other biotechnologies, is evolving but still remains very heterogeneous and often contradictory.

The present study encapsulates an overview of the legislative landscape within the genomic law and the security of genetic information domain across the 28 European Union member countries. Within the EU, certain member states encounter a regulatory void in this domain; nevertheless, our initiative strives to offer a comprehensive portrayal of both general and specific frameworks, ethical indicators, and overarching statutes that, despite their breadth, fail to encompass the entirety of genomic law.

Conclusion. Upon meticulous investigation, the author deduces the exigency for timely regulatory intervention to preclude potential perils arising from the utilization of artificial intelligence in the automated processing of personal data inclusive of genetic information. In the midst of the ongoing technological revolution, it becomes imperative to underscore the gravity of safeguarding personal data pertinent to human genome research in the cyberspace milieu, thus forestalling any regressions towards eugenics and mandating the adoption of ethical and legal norms by nation-states.

References

1. Clayton E. W., Evans B. J., Hazel J. W., Rothstein M. A. The law of genetic privacy: applications, implications, and limitations // Journal of Law Bioscience. 2019. Vol. 6(1). Pp. 1–36.

2. Danelyan A.A., Gulyaeva E.E. Actual problems of legal regulation of genomic research at the universal and regional levels // International Legal Courier. 2021. № 6. Pp. 16-37.

3. Danelyan A. A., Gulyaeva E. E. International legal aspects of cybersecurity // Moscow Journal of International Law. 2020. № 1. Pp. 44–53.

4. Dupan A. S. A New Paradigm of Personal Data Protection and Management. Moscow, 2016. 127 p.

5. Furrow B., Greaney T., Johnson S., Jost, T., Schwartz R. Bioethics: Health Care Law and Ethics (American Casebook Series). West Academic Publishing, 2013.

6. Gromova E. A., Petrenko S. A. Quantum Law: The Beginning // Journal of Digital Technologies and Law. 2023. Vol. 1(1). Pp. 62–88.

7. Guliaeva E. E., Trikoz E. N. Legal aspects of genetic research in Latin American countries (experience of forensic genetics in Argentina) // International Legal Courier. 2020. № 3–4. Pp. 56–60.

8. Leenen H. J. J., Pinet G., Prims A. V. Trends in health legislation in Europe. Paris: Masson for the WHO, 1986.

9. Schwab Klaus Martin. Technologies of the Fourth Industrial Revolution. Shaping the Fourth Industrial Revolution, 2018. 320 p.

10. Shestakova I. G. New temporality of digital civilization: the future has already come // Humanities and Social Sciences. 2019. Vol. 10. Pp. 26–29.

11. The interstate standard DIN ISO/IEC 17788-2016. URL: https://www.en-standard.eu/din-iso-iec-17788-information-technology-cloud-computing-overview-and-vocabulary-iso-iec-17788-2014/

12. Trikoz E. N., Gulyaeva E. E. Positions of the ECtHR on some issues of bioethics and genetic data // Advances in Law Studies. 2018. Vol. 6. Pp. 36–40.

13. Trikoz E. N. Protection of human rights in the context of the development of bioethics and genomics (review of international roundtable) // Bulletin of Peoples' Friendship University of Russia. 2019. Vol. 23. Pp. 141–154.

14. UN Russian-American resolution on cybersecurity. URL: https://russiaun.ru/en/news/1com202112021

O. Y. Latyshev,
PhD, Candidate of Philology, full member of IAS,
MAE, EAE, ISA, IOO AD SUTC,
Corr. member of MAPS,
Professor of RAE, President
Professor of Cypress University
M. Luisetto,
PhD, Honorary Vice-President,
International Mariinsky Academy
named after M. D. Shapovalenko,
Piacenza
P. A. Latysheva,
Executive Director,
International Mariinsky Academy
named after M. D. Shapovalenko

DIGITAL ENVIRONMENT AS AN INTEGRATIVE BEGINNING OF THE DEVELOPMENT OF DOCUMENTAL APPROACHES TO THE POSTULATION OF THE LEGAL STATUS OF THE PERSON

Abstract. The article is devoted to the study of key approaches to adequately determining the legal status of an individual, dictated by the nature of the digital transformation process. It examines the influence of the digital transformation process on the nature of postulating the legal status of an individual. This study is based on the works of S. S. Alekseev, A. K. Zharova, I. M. Rassolov, G. L. A. Hart and other authors.

Keywords: law, digital technologies, legal status of a person, telecommunications, internet, network, information and communication technologies

ЦИФРОВАЯ СРЕДА КАК ИНТЕГРАТИВНОЕ НАЧАЛО ВЫРАБОТКИ ДОКТРИНАЛЬНЫХ ПОДХОДОВ К ПОСТУЛИРОВАНИЮ ПРАВОВОГО СТАТУСА ЛИЧНОСТИ

Аннотация. Статья посвящается изучению ключевых подходов к адекватному определению правового статуса личности, продиктованных характером процесса цифровой трансформации. Проводится исследование влияния процесса цифровой трансформации на характер постулирования правового статуса личности. В основу данного исследования положены работы С. С. Алексеева, А. К. Жаровой, И. М. Рассолова, Г. Л. А. Харта и других авторов.

Ключевые слова: право, цифровые технологии, правовой статус личности, телекоммуникации, Интернет, сеть, информационно-коммуникационные технологии

Introduction. The category of “constitutional and legal status” is one of the most controversial categories in modern domestic jurisprudence, since due to changing conditions, it is simply impossible to form a unified approach to the definition. At the same

time, the category of "constitutional and legal status" is a key category in the domestic theory of modern law, in which all the main achievements of legal science and its accompanying practice are concentrated.

In the process of determining individual and collective rights and freedoms, the established constitutional and legal status makes it possible to achieve the optimal level of legal regulation, which determines the range of lawful actions of subjects of law in the field of adequate implementation of social relations.

It also becomes necessary to complete and timely legal assessment of the consequences of the implementation of this organic set of social relations, which, thanks to the concept of an internal point of view belonging to G.L.A. Hart, is determined by the nature of the relations of subjects of law [1. P. 5].

The definition of the constitutional and legal status of an individual arises in the process of the emergence of social relations in a digital telecommunications environment, in direct proportion to the nature of the functioning of rights in it. The position of the constitutional and legal status of the individual in the doctrine of modern domestic law is determined by the leading role of the state, which is realized, first of all, in the field of establishing the rights and obligations of each individual.

Along with this, the issues of determining the constitutional and legal status of a person in a digital communications environment are resolved in the direction of the process of ensuring guarantees and fulfilling the competencies of each subject of such relations [2. P. 21].

The main part of the article

In this case, it is the totality of the properties of the modern digital communications environment that acts as a prerequisite for the effective implementation of the constitutional and legal status of the individual and the legal regulation of the telecommunications environment.

Based on the generalization of the definitions of the digital telecommunications environment, the following characteristics of it should be distinguished, which are important for the constitutional and legal status of the personality of the subject of public relations in it [3. P. 12].

In the global telecommunications network, which is a technological platform, the development of public relations takes place through the distribution of documentation based on program documents [4. P. 53].

At the same time, it should be noted that considering the digital communications environment as a special self-developing social structure can significantly update the process of using a wide range of modern sociological and philosophical studies by domestic and world legal science;

At the same time, the position of a system that has signs of autopoiesis on the basis that it reproduces all the elementary parts traditionally belonging to it becomes characteristic for the digital telecommunication environment.

It performs such manipulations with the help of an organic combination of similar elements, and thanks to this, it acquires the ability to distinguish itself from the external environment, which is most typical for the most massive Internet resources [5].

Such expressions of the digital telecommunications environment, according to currently widespread forecasts of its most likely direction of development, will consistently and progressively acquire global significance. Such expressions of the digital telecommunications environment, according to currently widespread forecasts of its most likely direction of development, will consistently and progressively acquire global significance.

In the future, this property can be extended to the entire space of the digital telecommunications environment, and be realized in it in the form of communication, implying the functioning of this environment as a social system [5. P. 7].

In principle, the property of autopoiesis is also realized in the form of life, and in the form of consciousness, characteristic, in this case, of initiative and responsible users of this digital branched telecommunication environment.

The law in this case becomes, in relation to the digital telecommunications environment, to a certain extent, the "external environment", which the digital environment as a self-organizing system gradually begins to ignore.

This happens precisely because in the digital telecommunication environment, its own rules of regulation are formed, which are to a high degree determined by the own original mechanisms of this self-reproducing system. The question of the implementation of the constitutional and legal status of the individual in the digital communications environment acquires a fundamentally new sound due to the special influence of the properties of multiplying information.

It should be noted that the process of information multiplication in the digital communications environment seems impossible to stop the spread, otherwise the information system itself will be destroyed.

The influence of the principle of net neutrality, actively postulated within the digital telecommunications environment, is also undeniable, which implies that any information, regardless of its legal value, is considered equally important.

It is impossible not to mention the significant influence of the technological features of the digital telecommunications environment, in particular, the so-called "digital footprint" left by each user in it.

For the virtual space, the technological features of the digital communications environment are natural conditions, due to which they entail the question of the realization of natural human rights in a digital environment.

At the same time, jurists are faced with the following dilemma: should the regulatory norms that have already been formed within the digital telecommunications environment, which has the properties of an autopoietic system, be legalized?

Under this condition, additional guarantees should be provided to all participants in the digital telecommunications environment, without exception, otherwise the rules should be introduced in the traditional way, which can lead to a double risk.

Firstly, this is the risk of violating the digital communications environment itself, and secondly, which is no less, if not more important, the risk of an inevitable decrease in the authority of law due to an attempt to violate internal system rights.

Let us assume that the existence of a digital communications environment is taken into account as a system that is built on a contractual basis, as a result of which the

distribution of domain names and the corresponding connection to the Internet telecommunications network was made.

In this case, at the same time, one should also assume the existence of strong private legal mechanisms within the digital telecommunications environment, whose activities are aimed at regulating social processes. However, in the conditions of Russia and many foreign countries, it is administrative and legal means that have a serious impact on the digital environment.

In addition, the dependence of subjects of natural law on the terms of user and similar agreements that are not in essence contracts of accession cannot be overlooked, since they cannot be subject to any adjustment in accordance with the interests of any parties joining this agreement [6. P. 179].

S. S. Alekseev identifies such elements of the constitutional and legal status of the individual as legal personality, basic rights and obligations of subjects. In turn, the researcher attributes to the elements of the legal status of the individual the specific rights and obligations of the person, which are directly related to the presence of certain legal facts [7. P. 142].

Conclusion. Doctrinal approaches, which are currently being implemented in relation to the legal status of the personality of a citizen of the Russian Federation, in the digital environment require sufficient improvement in relation to the existence of a modern subject, which is traditionally called upon to act in a telecommunications environment.

References

1. Hart G. L. A. The concept of law / trans. from English; under general ed. E.V. Afonasina and S.V. Moiseeva. Saint Petersburg: Publishing house St. Petersburg. University, 2007. 120 p.

2. Zharova A. K. Law and information conflicts in the information and telecommunications sphere: monograph. Moscow: Janus-K, 2016. 230 p.

3. Rassolov I. M. Law and the Internet. Theoretical problems. 2nd ed., add. Moscow: Norma, 2009. 320 p.

4. Okinawa Charter for the Global Information Society // Diplomatic Bulletin. 2000. № 8. Pp. 51–56.

5. Luhmann N. The Autopoiesis of social systems. Essays on self-reference. New York: Columbia University Press, 1990. 340 p.

6. Alekseev S. S. Structure of Soviet law. Moscow: Legal. lit., 1975. 579 p.

7. Alekseev S. S. General theory of law. Moscow: Legal. lit., 1982. 320 p.

O. Y. Latyshev,
PhD, Candidate of Philology, full member of IAS,
MAE, EAE, ISA, IOO AD SUTC,
Corr. member of MAPS,
Professor of RAE, President
Professor of Cypress University
M. Luisetto,
PhD., Honorary Vice-President,
International Mariinsky Academy
named after M. D. Shapovalenko,
Piacenza
P. A. Latysheva,
Executive Director,
International Mariinsky Academy
named after M. D. Shapovalenko

FORMATION OF THE CONCEPTUAL AND CATEGORICAL APPARATUS WHEN FIXING THE LEGAL STATUS OF A PERSON IN THE DIGITAL ENVIRONMENT

Abstract. The work is devoted to studying the process of formation of a conceptual-categorical apparatus when consolidating the legal status of an individual in the digital environment. The research is carried out in the direction of determining the nature of the influence of the process of formation of the conceptual-categorical apparatus on the nature of consolidating the legal status of an individual in the digital environment. This study is based on the works of I. L. Bachilo, N. A. Vlasenko, N. M. Korkunov and other authors.

Keywords: law, digital technologies, legal status of a person, telecommunications, internet, network, information and communication technologies

ФОРМИРОВАНИЕ ПОНЯТИЙНО-КАТЕГОРИАЛЬНОГО АППАРАТА ПРИ ЗАКРЕПЛЕНИИ ПРАВОВОГО СТАТУСА ЛИЧНОСТИ В ЦИФРОВОЙ СРЕДЕ

Аннотация. Работа посвящена изучению процесса формирования понятийно-категориального аппарата при закреплении правового статуса личности в цифровой среде. Исследование проводится в направлении определения характера влияния процесса формирования понятийно-категориального аппарата на характер закрепления правового статуса личности в цифровой среде. В основу данного исследования положены работы И. Л. Бачило, Н. А. Власенко, Н. М. Коркунова и других авторов.

Ключевые слова: право, цифровые технологии, правовой статус личности, телекоммуникации, Интернет, сеть, информационно-коммуникационные технологии

Introduction. One of the most pressing problems currently existing within the framework of modern lawmaking, and the rapid development of the digitalization of society, should be the search for the most acceptable approaches to enshrining in the legislation the entire organic set of terms that are somehow related to the development of public relations in the digital telecommunications environment.

In particular, of particular interest among domestic and foreign lawyers is the process of forming a conceptual and categorical apparatus when fixing the constitutional and legal status of an individual in a digital telecommunications environment. First of all, this issue directly concerns the subjects whose activities are supposed to be regulated in the course of their daily work in the digital telecommunications environment.

At the same time, the focus of attention of domestic and foreign lawyers developing modern legislative initiatives is the constitutional legal status of the personality of such subjects. The reason for this provision should be called the fact that it is through the legislative definition that the place and significance of each entity participating in the digital communications environment should also be determined.

Results. A circumstance of fundamental importance in this case is the need for a correct and timely determination of the place of the entire organic set of subjects of the digital communications environment in the system of public relations.

So, for example, I. L. Bachilo comes to the conclusion that an organic set of concepts and categories designed to determine the legal status of subjects of the digital communications environment has a backbone value [1. P. 14].

At the same time, from the point of view of this study, this set of concepts and categories should also determine the subject area of interests and actions of the subjects of the initiative activity of the digital telecommunications environment.

Along with this, according to I. L. Bachilo, one should also think in a timely manner about their appropriate use in the fast-flowing process of forming various semantic forms of concepts and categories designed to determine the rights, obligations and powers of the subjects of the digital telecommunications environment.

These can be glossaries, thesauri, dictionaries and encyclopedias, and each such categorical-conceptual tool will actively contribute to the emergence of due certainty in this area of rights. At the same time, it should be noted that, according to a rather productive idea of the constitutional and legal status of an individual, any definition of a given subject is one of its properties.

In the idea of the constitutional and legal status of the individual, an inextricable and highly productive connection of the idea of universality with the idea of subjectivity is carried out, with the inherent intentional ability to construct an object [2. P. 8].

At the same time, in the modern jurisprudence literature, an increasingly growing backlog of law and legislation is ascertained from the pace that is directly characteristic of the development of technologies and social relations.

The rapid and widespread introduction of technological innovations in various fields of human activity leaves practically no worthy place for generally accepted methods of legal technique in order to successfully and quickly overcome new problems.

For the law-making process, as it has been for quite a long time, the new digital realities also practically do not leave the place occupied by new law-making algorithms.

These problems are connected, first of all, with the determination of the constitutional and legal status of the personality of the key and influencing actors in the development of the digital telecommunications environment. The law in such an unusual situation is predominantly involved not so much in prevention as in resolving the adverse consequences of the misuse of the digital telecommunications environment, which, as a rule, inevitably have a so-called delayed effect.

Due to this circumstance, such consequences cannot be predicted, first of all, even by the developers of new information and communication technologies, on which the daily functioning of the digital communications environment is based.

Moreover, the occurrence of negative consequences of the misuse of the digital communications environment cannot be predicted with a sufficient degree of certainty by users or law enforcers.

On this basis, it should be suggested that the possibility of the occurrence in this connection of the detrimental consequences of the misuse of the digital communications environment can actively and quite variably contribute to the emergence of legal uncertainty as well.

The state of legal uncertainty presupposes the existence in the space of the digital communications environment of subjects of newly built public relations in the field of informatisation. It seems necessary to state that the state of legal uncertainty finds its manifestations in the absence of a clear definition, which does not allow unambiguously and timely establishing the existence of the addressee of legal norms [3. P. 9].

Along with this, it is not yet possible to introduce adequate rights and obligations in a state of legal uncertainty, which form the core of the constitutional and legal status of the individual.

Among other things, the state of legal uncertainty gives rise to a simultaneous discrepancy between rights and duties, and a simultaneous discrepancy between duties and rights. This circumstance violates the dialectical law of the unity of opposites, as a result of which the systematic functioning of the constitutional and legal status of the individual is still problematic.

As a result of the emergence of a state of legal uncertainty, the system-forming meaning, which is traditionally characteristic of concepts and categories, is replaced by a situational one. At the same time, the situational significance of concepts and categories makes it possible, at best, to single out in a given situation a special subject that functions in the general mass of actors.

Such a selection of a special subject makes it possible to designate its inherent special place and role in the system of constantly and productively developing social relations.

At the same time, it should be remembered that such concepts as “state”, “place” and “role” are already included in the dictionary definition of “status” as such, which sufficiently allows us to simultaneously analyze the “constitutional and legal status”, which still continues to inevitably remain a pronounced debatable category in modern jurisprudence.

However, it seems necessary to assume that in the course of the progressive development of modern jurisprudence, supported by progressive authors of legislative initiatives, the current position of “constitutional legal status” will be defined much more clearly [4].

Conclusion. The most convincing and pronounced trends, according to the process of unambiguous dominance of which the formation of key units of the conceptual and categorical apparatus takes place in the course of securing the legal status of an individual in the digital environment, consists, first of all, in the rapid advance of rapidly developing technologies of the capabilities of the currently functioning legal system of the country and peace.

References

1. Bachilo I. L. On terms and concepts in law // Questions of jurisprudence. 2014. No. 3. Pp. 14–23.

2. Vlasenko N. A. Theory of state and law: scientific and practical guide. Moscow: Prospekt, 2009. 230 p.

3. Korkunov N. M. Lectures on the general theory of law. SPb.: Legal. Center Press, 2003. 120 p.

Mailin Ramos Morales,
Masters in Social Studies of Science and Technology,
Specialist in Criminal Sciences,
Assistant Professor,
University of Cienfuegos "Carlos Rafael Rodríguez"
Yoruanys Suñez Tejera,
Doctor of Legal Sciences,
Lawyer at the Cienfuegos Collective Law Firm,
Professor,
University of Cienfuegos "Carlos Rafael Rodríguez"
Rachel Domínguez Suñez,
student,
University of Cienfuegos "Carlos Rafael Rodríguez"

ARTIFICIAL INTELLIGENCE AND THE ADMINISTRATION OF JUSTICE IN CUBA

Abstract. In regards to the topic of Artificial Intelligence (AI), one can appreciate that it is no longer part of a distant future that could only be dreamed of by reading science fiction works. In the world, and in Cuba, it is already a tangible and exciting phenomenon that makes its analysis and development necessary to achieve advances in the social and economic life of the country, and thus ultimately achieve an increase in the well-being and progress of society. One cannot remain motionless in the face of the constant technological change that influences most human activities. This includes the law, where the application of technology has increased efficiency and effectiveness in very specific areas such as, for example, the fight against fraud and irregularities. Nonetheless, the legal challenges presented by AI are many, and in such diverse areas as personal data protection, equality, legal security, transparency and accountability, among others.

Keywords: Artificial Intelligence, Administration of Justice, Development, Digital Transformation, Judicial processes, Criminal Law, Technological change

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОТПРАВЛЕНИЕ ПРАВОСУДИЯ НА КУБЕ

Аннотация. Искусственный интеллект уже не является частью далекого будущего, о котором можно только мечтать, читая научно-фантастические произведения. В мире и на Кубе это уже ощутимое и захватывающее явление, анализ и развитие которого необходимы для достижения прогресса в социальной и экономической жизни страны, а значит, в конечном счете для повышения благосостояния и прогресса общества. Нельзя оставаться неподвижным перед лицом постоянных технологических изменений, которые влияют на большинство видов человеческой деятельности. Это касается и юриспруденции, где применение технологий позволило повысить эффективность и результативность в весьма специфических областях, таких как, например, борьба с мошенничеством и нарушениями. Тем не менее правовых проблем, связанных с применением искусственного интеллекта, немало, причем в таких разных областях, как защита персональных данных, равенство, правовая безопасность, прозрачность и подотчетность и др.

Ключевые слова: искусственный интеллект, отправление правосудия, развитие, цифровая трансформация, судебные процессы, уголовное право, технологические изменения

Introduction. When speaking about artificial intelligence in Cuba, it is necessary to point out that since the late 1980s the topic has been approached with interest by researchers in scientific centers and universities, but always from an academic point of view. In comparison to other technological areas, AI, although it is applied in a limited way, has not reached predominance in Cuban society. The improvement of information processing capabilities and the desire to enhance the development and optimization of processes has motivated the Cuban government to reflect on the urgent need to draw up strategies to enhance the development of artificial intelligence [9].

Main part. In February 2023, members of the highest levels of the Cuban government, including President Miguel Díaz-Canel, met with representatives of the Cuban Academy of Sciences (ACC) to reflect on AI within the context of digital transformation for development. Among the difficulties, the academics highlighted the few Cuban computer products or services developed with AI techniques for solving problems, the fact that there are few opportunities to develop a professional career in this field and the lack of a national strategy to coordinate these efforts. It was also clear from the beginning that the development of AI could not be seen without clear ethics and rules, at both the national and international level. In addition, it was specified that to create Cuban AI-based solutions, the correct use of data would first be necessary. In this regard, Member of Merit and Coordinator of natural and exact sciences of the ACC, Luis Montero Cabrera, mentioned that the foundation of the massive use of Artificial Intelligence is in the achievement of a systemic, stable, actionable database, which encompasses the country in full [8].

The Cuban president Miguel Díaz Canel has stated that an Artificial Intelligence Strategy is already being worked on, but that it is vital to work on the interconnection of

artificial intelligence with the production of goods and services, public administration, and the territories. Furthermore, it is necessary to cover the topic of the organization, structure and management of data because Cuban society needs to achieve the implementation of AI to promote the formation and training of human capital associated with Big Data and Artificial Intelligence for their correct use in public and business management. Additionally, the relationship on these issues between universities, companies and the government must be strengthened [8].

In mid-2023 a group of experts met at the National Union of Jurists of Cuba to address the discussion on the Strategy for the Development of Artificial Intelligence in Cuba. At this meeting, Pedro Piñero Pérez, a member of the project that currently creates it, explained that it is necessary to use a multidisciplinary approach in which both the natural and social sciences address the issue of intelligent systems, because without this approach the strategy would not fit into current Cuban society. The draft strategy has several commissions of experts in various subjects, as well as the participation of Cuban and foreign universities, research centers, the collaboration of the United Nations Educational, Scientific and Cultural Organization (UNESCO) and the Ministry of Justice for the ethical use of AI [8].

The limitations presented in the field of technology in Cuba are compensated in a certain way by the opportunities offered by having highly qualified professionals. Furthermore, the approximately 2,292 investigations in the Scopus database are evidence of the interest that the Cuban scientific community has in the subject. Another fundamental element is the cooperation with several countries such as Italy, Canada, the United States, Colombia and the Netherlands, particularly for research development. For example, the Ministry of Communications of Cuba, as part of its cooperation with China, created the Project for the Creation of the International Institute of Artificial Intelligence Research at the University of International Studies of Hebei in 2019. The Cuban side is directed by the University of Camagüey, although other higher education centers such as UCI, CUJAE and Marta Abreu University participate [8].

Nonetheless, when analyzing the application of AI in the administration of justice in Cuba, we see that there are still many opportunities that have not been exploited and that can facilitate and streamline the processes. Such systems are being developed in countries such as Spain, where remarkable results are being shown in their use. In her judicial processes report, Cristina Lorenzo Pérez, [6] lawyer at the Spanish Ministry of Justice, performs an extensive examination on the implementation of intelligent systems and tools that facilitate the development of the administration of justice in Spain. Some of these applications, in the opinion of the authors, could be applied in Cuba, such as the ones presented below:

Automatic cancellation of criminal records

The use of this system would help a person not to have to request the cancellation of the record to which he is entitled if he meets the requirements established in the criminal code and would also allow for status updates in the criminal records system. This could be useful, for example, when agreeing to the suspension of a prison sentence, since those criminal records that have been canceled, or should have been, will not be taken into account. The result would be a great contribution in updating the register of

sanctioned persons with almost no human intervention, an element so necessary for the Cuban legal system that is sometimes overloaded due to lack of personnel [6].

Textualization of views

This is a solution provided by artificial intelligence using audios or videos that are recorded during hearings or statements, through which text is automatically generated. This system would facilitate the work of judges and judicial personnel, so that they could analyze the hearings they conduct more quickly, in addition to being able to perform specific searches on interventions that need to be specified, such as names, places or quantities that could be referred to in the hearing [6].

Legal voice dictation

This is a legal voice transcription system which directly benefits the productivity of legal operators. An example of this could be a judge who uses this tool to dictate his conclusions, notes and resolutions, allowing him to draft judgments, extracts, orders or considerations on his computer faster. This tool is able to recognize the technical legal language used by legal operators and even perform automatic and simultaneous translation into another language [6].

360 Search Engines

This tool allows for the transcription of hearings, making it possible to locate information associated with files, classify terms depending on the number of times they are found in the text to be analyzed, and optimize the time spent by the judge in the analysis of the document. In countries such as Spain, advanced documentary search engines are being developed that include semantic search functions. Through this system it will be possible to search by writing or natural language all the documents of the procedural management system, even the archived ones [6].

Conclusion. All this would constitute an improvement in the results of the judicial administration system, providing greater security inside and out and improving communication with the subjects of judicial decisions. Although we already see this type of results in many countries that to a greater or lesser extent use intelligent systems in the administration of justice, Cuba has lagged behind in the use of it, so there is still a way to go to achieve the wide range of benefits that the use of AI brings in the administration of justice.

References

1. Aspis A. Las TICs y el Rol de la Justicia en Latinoamérica // Derecho & Sociedad Journal. 2010. № 35. Pp. 327–340.

2. Barona Vilar S. Inteligencia artificial o la algoritmización de la vida y de la justicia: ¿solución o problema? // Journal Boliviana de Derecho. 2019. № 28. Pp. 18–49.

3. Barona Vilar, S. Agoritmizacion del Derecho y la Justicia. De la Inteligencia Artificial a la Smart Justicie. Ed. Arazandi, 2021. 230 p.

4. Beiro Magan J. Retos tecnológicos de la Administración de Justicia española para la tercera década del siglo XXI. URL: https://pensamientocritico.sisej.com/retos-tecnologicos

5. Lang Irrazábal M. La inteligencia artificial en la administración de justicia // Ars Iuris Salmanticensis, Tribuna de actualidad. 2020. Vol. 10. Pp. 2340–5155.

6. Lorenzo Pérez C. Inteligencia Artificial en la administración de justicia: Regulación española y marco europeo e internacional // Proyectos desarrollados por el ministerio de justicia en España. 2022. Vol. 7. Pp. 13–26.

7. Suarez X., Paulo R. El Reto de la Regulación de la Inteligencia Artificial en el Sistema Judicial y su Entorno // Journal Jurídica Portucalense. 2022. Vol. 2. Pp. 145–156.

8. Ureña, René, ¿Máquinas de justicia?: Inteligencia artificial y sistema judicial en América Latina. URL: https://agendaestadodederecho.com/maquinas-de-justicia-inteligencia-artificial-y-sistema-judicial-en-america-latina

9. Jalón Arias E., Ponce Ruiz D., Arandia J. C., Arrias Añez J. C. Las limitaciones de la aplicación de la inteligencia artificial al derecho y el futuro de la educación jurídica // Journal Conrado. 2021. Vol. 17(83). Pp. 439–450.

10. Vida Fernández J. Los retos de la Regulación de la IA: algunas aportaciones desde la perspectiva europea // Sociedad digital y Derecho. 2018. Vol. 6. Pp. 203–224.

E. A. Pogosyan,
Senior lecturer,
Ryazan State University named after Yesenin

DIGITAL TECHNOLOGIES AND THEIR IMPACT ON THE LEGAL LANDSCAPE

Abstract. The rapid advancement of digital technologies has ushered in an era of unprecedented transformation across various sectors, and the legal domain is no exception. This article delves into the intricate interplay between digital technologies and the field of law. It examines the multifaceted influence of digital technologies on legal processes, jurisprudence, and the administration of justice. Through an exploration of key areas such as electronic evidence, online dispute resolution, data privacy, and the emergence of blockchain technology, this article sheds light on the complex challenges and opportunities presented by the digital era within the legal realm.

Keywords: digital technologies, legal landscape, legal systems, legal principles, Blockchain technology, the principles of justice, the rule of law

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИХ ВЛИЯНИЕ НА ЮРИДИЧЕСКИЙ ЛАНДШАФТ

Аннотация. Стремительное развитие цифровых технологий положило начало эпохе беспрецедентных преобразований в различных отраслях, и юридическая сфера не является исключением. В данной статье рассматривается сложное взаимодействие цифровых технологий и сферы права. В ней исследуется многогранное влияние цифровых технологий на юридические процессы, судебную практику и отправление правосудия. Исследуя такие ключевые области, как электронные доказательства, разрешение споров в режиме онлайн, конфиденциальность данных и появление технологии блокчейн, статья проливает свет на сложные проблемы и возможности, которые открывает цифровая эра в правовой сфере.

Ключевые слова: цифровые технологии, правовой ландшафт, правовые системы, правовые принципы, технология блокчейн, принципы правосудия, верховенство права

The convergence of digital technologies with the legal landscape has ushered in a paradigm shift, altering the way legal professionals navigate, interpret and apply laws. This article embarks on an exploration of the profound impact that digital technologies have on various dimensions of law and how legal systems adapt to this evolving digital ecosystem.

One of the pivotal arenas where digital technologies intersect with law is electronic evidence. The digitization of information has revolutionized the presentation and analysis of evidence in legal proceedings. Digital forensics, encompassing techniques to extract, preserve, and analyze electronic data, has become an indispensable tool in investigations and litigation [5. Pp. 215–230]. The authenticity and admissibility of digital evidence pose new challenges that necessitate a thorough understanding of technological intricacies.

Electronic evidence demands a harmonious collaboration between legal practitioners and digital experts to ensure a seamless integration of technology in the judicial process.

The advent of digital technologies has catalyzed the development of Online Dispute Resolution mechanisms, providing an alternative platform for resolving conflicts in the virtual realm. ODR platforms leverage technology to facilitate mediation and arbitration, transcending geographical barriers and enhancing access to justice [2. Pp. 345–363]. However, the effectiveness of ODR raises questions about procedural fairness, enforcement of decisions, and the preservation of due process rights.

Online Dispute Resolution presents a promising avenue for enhancing dispute resolution accessibility, while also prompting a reevaluation of traditional legal principles in the digital context.

The proliferation of digital technologies has given rise to intricate challenges concerning data privacy and cybersecurity. Legal frameworks, such as the General Data Protection Regulation (GDPR), strive to safeguard individuals' data in an increasingly interconnected world [4. Pp. 89–105]. Balancing the imperative to protect privacy with the utility of data-driven innovations calls for a delicate equilibrium between legal safeguards and technological advancements.

The intersection of data privacy laws and digital technologies necessitates a dynamic approach to address emerging privacy concerns in the digital age.

Blockchain technology, characterized by its decentralized and immutable nature, has disrupted traditional legal concepts through the advent of smart contracts. These self-executing contracts are encoded on blockchain networks, automating the enforcement of contractual obligations [1. Pp. 457–485]. While blockchain holds potential for enhancing transparency and reducing transaction costs, legal challenges such as jurisdictional issues and enforceability remain pivotal areas of exploration.

Blockchain technology introduces novel possibilities for contractual relationships, prompting legal scholars to navigate the uncharted waters of blockchain jurisprudence.

Artificial Intelligence (AI) has permeated legal practice, empowering legal professionals with tools for legal research, document review, and predictive analytics. The integration of AI raises ethical dilemmas, including bias in algorithms and the implications of delegating decision-making to machines. The coexistence of human judgment and AI-generated insights shapes the future landscape of legal expertise [3. Pp. 311–313].

The symbiotic interaction between human legal practitioners and AI technologies underscores the need for ethical guidelines and a nuanced understanding of AI's role in legal proceedings.

As digital technologies continue to redefine legal parameters, regulatory challenges emerge as a critical facet. The evolution of digital technologies often outpaces the formulation of adequate legal frameworks [6. Pp. 495–506; 7]. This disjuncture necessitates a proactive approach to adapt existing laws and develop novel regulations that align with the dynamic digital landscape.

The coevolution of digital technologies and legal regulations requires an agile legal framework capable of fostering innovation while preserving fundamental rights.

The fusion of digital technologies with the legal domain ushers in an era of unparalleled transformation and complexity. As legal systems grapple with the challenges and opportunities presented by the digital age, a comprehensive understanding of electronic evidence, online dispute resolution, data privacy, blockchain technology, AI, and regulatory dynamics becomes paramount. Navigating this intricate terrain requires legal scholars, practitioners, and policymakers to embark on a collective journey to harness the potential of digital technologies while upholding the principles of justice and the rule of law.

References

Chen L., Lee D. Blockchain and Smart Contracts: A Legal Perspective // Harvard Journal of Law & Technology. 2017. No. 30(2). Pp. 457–485.

Cortes A. Online Dispute Resolution: Challenges and Opportunities // International Journal of Law and Technology. 2019. Vol. 23(3). Pp. 345–363.

Crawford K., Calo R. There is a Blind Spot in AI Research // Nature News. 2016. Vol. 538(7625). Pp. 311–313.

Gromova E. A., Petrenko S. A. Quantum Law: The Beginning // Journal of Digital Technologies and Law. 2023. Vol. 1(1). Pp. 62–88.

Johnson M. Data Privacy in the Digital Age: Navigating Legal and Ethical Challenges // Journal of Cybersecurity and Privacy. 2019. Vol. 7(1). Pp. 89-105.

Smith R. Electronic Evidence in Legal Proceedings: A Technological Perspective // Journal of Digital Law. 2020. Vol. 12(2). Pp. 215–230.

Zittrain J. The Challenges and Opportunities of Regulation in a Digitally Transformed World // The European Review. 2018. Vol. 26(4). Pp. 495–506.

A. Sh. Sodikov,
PhD, Associate professor,
Tashkent State University of Law

ARTIFICIAL INTELLIGENCE BANNED OR SUPPORTED IN ISLAMIC LAW?

Abstract. This descriptive scientific article shortly analyzes the intersection of artificial intelligence (AI) and Islamic morality, discussing the potential impact of AI on ethical considerations within the framework of Islamic law. It explores the opportunities and challenges that arise when integrating AI systems in line with Islamic moral values. This article aims to stimulate discussion and guide future research concerning the harmonious integration of AI and Islamic law.

Keywords: artificial intelligence, Islamic morality, ethics, principles, privacy, fairness, sharia

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ЗАПРЕЩЕН ИЛИ ПОДДЕРЖИВАЕТСЯ В ИСЛАМСКОМ ПРАВЕ?

Аннотация. В статье кратко анализируется пересечение искусственного интеллекта и исламской морали, обсуждается потенциальное влияние искусственного интеллекта на этические соображения в рамках исламского права. В нем исследуются возможности и проблемы, возникающие при интеграции систем искусственного интеллекта в соответствии с исламскими моральными ценностями. Целью этой статьи является стимулирование дискуссий и руководство будущими исследованиями, касающимися гармоничной интеграции искусственного интеллекта и исламского права.

Ключевые слова: искусственный интеллект, исламская мораль, этика, принципы, частная жизнь, справедливость, шариат

In recent years, artificial intelligence (AI) has become popular all over the world. Despite its many advantages, different legal families are taking different approaches to regulating AI. The impact of AI on ethics, the attitude of various sources of law to AI, the regulatory mechanism and other such issues are gaining urgent importance [18]. It is possible to cite many examples of the fact that such issues related to AI are clearly regulated in the families of common law and civil law, and various scientific studies have been carried out.

However, it can be observed that in countries where Islamic law rules, the issues of the interaction of AI and Sharia law norms have not been fully studied, and in some Arab countries even AI is prohibited. In addition, if we pay attention to various international scientific bases, it can be seen that there are very few scientific studies devoted to the issues of the interaction of Islamic ethics and AI. For instance, such researchers cannot be found in the jstor.org database. At a time when the issue of AI has become one of the most popular research topics in other countries, the development of AI has revived a long-standing debate about the relationship between modern liberalism and Islamic law [11].

As scientist A. Z. Ali mentioned, AI is a combination of computer science, philosophy and physiology. AI is a broad topic, consisting of different sphere, from machine vision to expert systems. The element that the sphere of AI have in common is the creation of machines that can "think". In order to classify machines as "thinking", it is necessary to define intelligence. To what degree does intelligence consist of, for example, solving complex problems, or making generalizations and relationships? And what about perception and comprehension? Research into the areas of learning, of language, and of sensory perception have aided scientists in building intelligent machines [1. P. 74].

In general, after having a brief description of AI, the impact of AI on Islamic law and the legal issues that may arise as a result of their interaction can be analyzed below:

Firstly, Islamic law does not reject artificial intelligence. After all, Sharia does not oppose the development of science. However, Muslims emphasize the value of upholding human dignity, compassion, and the quest of spiritual development while acknowledging the potential of AI. They issue a warning against placing an undue dependence on AI, which could cause morality and human contact to be neglected. In addition, unethically receiving various awards (in competitions, contests etc.) or evaluation (in educational institutions, etc.) through plagiarism or various (scientific, technical, creative, etc.) works prepared by AI is considered against Islamic ethics. In this case, moral issues such as not fulfilling the rights of other members of society, acting contrary to moral teachings, teaching members of society to "fraud" are considered as the first and main problem. Due to the fact that morality is at a lower level in other legal families, various legal issues [12] and judicial disputes [4] related to AI are observed only on the issue of plagiarism. However, the issue of the influence of AI on the morals of society members is not a cause for concern for other families of law, such as Sharia law.

Secondly, issues related to copyright infringement [4] are one of the most important issues in Islamic law, like other legal families. According to the rules of Sharia, not every author wants to be victim of copyright infringement by other people. However, AI technologies sometimes use the authors' work without their consent.

Thirdly, the issue of privacy is also considered a sensitive aspect in AI technologies. The right to privacy is a supreme value in Sharia law. The person, the honor, dignity, and personal secrets of the person are one of the main issues that are protected in the Islamic religion.

Although all the main issues mentioned above are common to Islamic law, the attitudes towards them by countries based on different Sharia rules are different. At this point, the following basic rules of Islamic law are applied in the regulation of the above-mentioned issues:

Firstly, the inextricable connection between morality and Islamic law. Islamic law emphasizes the permissibility of strict adherence to Sharia ethics in human relations with AI. In some countries, the unethical use of AI is subject to administrative and criminal liability, while in some countries, such actions are considered a "struggle against the evil" of individuals and do not impose strict punishments. However, most importantly, in almost all countries of Islamic law, the use of AI is primarily ordered not to harm other members of society, not to encroach on social morality and public order. Most importantly, AI is seen as a means of developing intellectual capabilities.

Secondly, copyright is also protected in Islamic law. Copyright promotes respect for the creator's property by others. Creativity (ideas, books, programs, designs, music, etc.) expressing the intellectual abilities of each person is recognized as property. It provides effective ways to address important regulatory compliance, protection and access to human intellectual activity, and ethical and legal advice in this area.

Some countries have raised such issues to a higher level and banned AI technologies, while others are creating AI development centers and spending huge resources to support them.

In the table below, you can see the situation of the Arab League countries in the example of Chat GPT.

Table 1

№	List of Arab League countries	Supporters and developers	Blocked or Banned
1	Egypt	+	
2	Sudan		+
3	Algeria	+	
4	Iraq	+	
5	Morocco	+	
6	Saudi Arabia	+	
7	Yemen		+
8	Syria		+
9	Somalia	+	
10	Tunisia	+	
11	Jordan	+	
12	United Arab Emirates	+	
13	Libya		+
14	Palestine	+	
15	Lebanon	+	
16	Mauritania	+	
17	Oman	+	
18	Kuwait	+	
19	Qatar	+	
20	Bahrain	+	
21	Djibouti	+	
22	Comoros	+	

As can be seen from the above list, AI (in the example Chat GPT) is used in all other 18 countries except for 4 Arab League countries (Sudan, Yemen, Syria, Libya). In addition, many new types of AI can be found in UAE, Saudi Arabia and Egypt. Even the position of consultant has been introduced in the state administration bodies regarding the application of AI.

In addition, the use of AI is prohibited in the countries of Afghanistan and Iran [15], where Sharia rules are applied. For example, you can observe that Chat GPT is banned in these countries.

Regarding the use of AI, if one turns to the Holy Qur'an, which is the main source of Islamic law, one can find many verses in the holy book about the use of scientific achievements.

According to the scholars (Yasmansyah, Lainah, Zulfani Sesmiarni) there are about 750 verses of the Qur'an that talk about the universe and its phenomena, and command humans to know and make use of it [17. P. 467].

For instance, "O company of jinn and humans! If you can pass through the confines of the heavens and the earth, then do pass through. But you will not pass through except by authority [from the God] [14. P. 795].

In the verse 47 of the Surah Hajj, "Have they not traveled throughout the land so their hearts may reason, and their ears may listen? Indeed, it is not the eyes that are blind, but it is the hearts in the chests that grow blind [14. P. 481]".

In accordance with N.Hikmah states that based on Surah Ar-Rahman can be concluded that: first, Allah gives freedom for jinn and humans to develop themselves and take advantage of the development of science and technology for quality development [6. P. 7].

Yasmansyah, Lainah, Zulfani Sesmiarni note that "Why should humans follow Divine instructions in producing and applying science and technology? That's because the knowledge and capacity of the human brain to accommodate the knowledge of Allah, as well as all human abilities are very limited" [17. P. 473].

Shaikh Mohd Saifuddeen states, "It is abundantly clear that the concepts related to ICT is not alien to Islam. What is apparent is that ICT goes hand-in-hand with the attainment of knowledge in that ICT makes it easier for us to gather, store, analyse and communicate information that can further be processed into valuable knowledge" [13. P. 65].

Isah Onuweh Jimoh emphasized "as we have seen, we have acknowledged that Qur'an addresses both Science and Technology. It is not that it is a book of Sciences but as the last testament to the whole universe, it ought to address all that are necessary for humanity of all ages in accordance with their level of understanding development" [9. P. 426].

Several jurists and scholars have conducted research on AI and Islamic law. The works of the following scholars are related to artificial intelligence and Islamic law:

It is possible to mention Professor of Islam and Biomedical Ethics Dr. Mohammed Ghaly (Qatar). He is known for his research on artificial intelligence and Islamic law at the Qatar College of Islamic Studies (Hamad bin Khalifa University). His works are aimed at distinguishing and coordinating the important teachings of AI and Islam [7].

Dr. M. Akif Aydın Osmanniye Korkut Ata Universiteti (OKMEV) is a professor at the Faculty of Law, known for the research work on AI and Islamic law (Turkey).

Dr. Nabil Sultan is a professor of Masriq Islom Universitetida, developed sophisticated analysis and opinion on artificial intelligence and Islamic law (Oman). His work includes separate perspectives on AI and Islamic law and covers issues of fairness, trust, ethics and intellectual property in law.

Dr. Osman Karatepe is a professor of Duzce Universiteti (Turkey). He is the author of scientific works on the research and coordination of the problems of artificial intelligence and Islamic law. His works on AI and Islamic law aim to provide a separate perspective and emphasize the importance of morality in Islamic law.

These scientists are just a few examples, and many other famous works in this field can be cited.

Many projects and grants related to the interaction of Islamic law and AI are also being implemented. In particular, in 2020, Facebook promised funds for the "Ethics in AI Research Initiative Asia Pacific" project [3]. However, if we pay attention to the list of winners [2] of this project, it can be observed that among them, the impact between AI and Sharia norms has not been fully and comprehensively researched.

Facebook's initiatives and projects aimed at strengthening independent research in these areas can be observed in many other examples. In particular, support for the TUM Institute for Ethics in AI [8] and similar initiatives are supported by Facebook in other countries and regions, such as India and Latin America.

The countries of the Arab League pay a lot of attention to the development of AI, and several centers have also been established. The following centers are of particular importance in helping the development of artificial intelligence in the Arab League countries:

Dubai AI Center is a unique Silicon Valley; It is the administrative center of AI development. This center conducts research on the study, development of innovative solutions for AI. The center includes conducting academic research and supporting start-up projects aimed at the development of AI.

Riyadh Center for Artificial Intelligence is located in Riyadh, Saudi Arabia. The center aims to facilitate the application and programming of artificial intelligence in the field of irrigation and water resources management.

Cairo AI Center is located in Egypt. This center is engaged in study, learning and research in the sphere of artificial intelligence.

However, information on the establishment of such AI centers in other 18 Arab League countries was not found. It can be concluded that the development of AI is being paid special attention in Saudi Arabia, where the Islam doctrine is considered the most strictly. In addition, the existence of AI centers in Egypt, where the most famous educational institutions for teaching Islamic teachings are located, is not difficult to understand that there is no strict opposition between AI and Islamic ethics.

In addition, three main countries mentioned above (UAE, Saudi Arabia, Egypt) use the experience of other developed countries to improve their AI based on various international conferences and roundtables. In particular, on 2 December 2021, in a roundtable discussion organized by Egypt's Ministry of Communication and Information

Technology in cooperation with the League of Arab States at the ITU and UNESCO Regional Digital Inclusion Week [10], they discussed the challenges and opportunities for the development of a common AI strategy for Arab States [16].

At this point, if we pay attention to Uzbekistan, where more than 90% of the population is Muslim: Although there is no specific law regulating AI in our country, the sphere is fully regulated by various normative legal acts. In particular, the following normative legal acts can be a clear proof of this.

Table 2

№	Titles of normative-legal acts	Data and number
1	"On the approval of the regulation on the establishment of a special regime for the support of artificial intelligence technologies and the procedure for its operation"	Resolution of the Cabinet of Ministers of the Republic of Uzbekistan, No. 717, adopted on 29.11.2021.
2	"On measures to introduce a special regime for the use of artificial intelligence technologies"	Resolution of the President of the Republic of Uzbekistan, No. 5234, adopted on 26.08.2021.
3	"On the establishment of the scientific-research institute for the development of digital technologies and artificial intelligence"	Resolution of the Cabinet of Ministers of the Republic of Uzbekistan, No. 475, adopted on 31.07.2021.
4	"On measures to create conditions for rapid introduction of artificial intelligence technologies"	Resolution of the President of the Republic of Uzbekistan, No. 4996, adopted on 17.02.2021.

Although the above-mentioned normative legal acts are clearly devoted to the issues of regulation of AI, in the process of their adoption, the issue of compliance with the laws of Sharia was not studied. Conclusions containing relevant opinions were not received from Islamic scholars.

At this point, if we pay attention to A. Z. Ali's opinion, Islamic studies of today demands a new theoretical foundation to address not only the authentic or traditional approach in addressing traditional sources but also the modern factors in teaching-learning processes which are very contemporary in nature [1. P. 78].

Summarizing all the above thoughts and views, the following conclusions can be drawn:

Islamic law, also known as Sharia law, provides a moral and legal framework for Muslims, guiding various aspects of life, including technological advancements like AI. While there is no specific body of law dedicated to regulating AI in Islamic jurisprudence, Islamic legal principles and ethical considerations can be applied to address the challenges and implications arising from AI technology.

Islamic law emphasizes ethical principles, such as justice, fairness, accountability, and the preservation of human dignity. These principles can be applied to guide the de-

velopment, and use of AI systems. Islamic scholars and jurists often evaluate the ethical implications of AI technologies to ensure adherence to these principles.

Islamic law requires adherence to Islamic values and doctrines. AI systems and applications need to align with these values, ensuring they are not used for purposes that are prohibited or unethical according to Islamic teachings. For instance, AI applications should avoid promoting or facilitating activities such as gambling, interest-based transactions, or promoting harmful content.

Islamic law recognizes the importance of privacy and condemns unwarranted surveillance. AI systems should be designed to respect privacy rights, ensuring that personal data is protected and not misused. Islamic legal principles can guide the development of AI systems that uphold privacy and prevent unauthorized access to personal information.

Islamic law emphasizes the importance of accountability in decision-making processes. AI systems must be transparent, explainable, and subject to oversight to ensure that, they do not undermine human accountability. Islamic legal principles can be applied to ensure that AI systems are accountable for their actions and decisions.

Islamic law prohibits causing harm to oneself or others. AI systems should adhere to this principle by avoiding biased decision-making, discrimination, or malicious activities. Islamic legal principles can be employed to address any potential harm caused by AI systems and provide remedies for affected parties.

It is important to note that the application of Islamic law to regulate AI is an ongoing discussion within Muslim-majority countries and Islamic scholarly communities. Efforts are being made to develop guidelines and frameworks that incorporate Islamic values into the ethical development and deployment of AI technologies while respecting the broader legal and regulatory landscape in each country.

References

1. Ali A. Z. A philosophical approach to artificial intelligence and Islamic values // IIUM Engineering Journal. 2011. Vol. 12, No. 6. Pp. 73–78.

2. Award Recipients. URL: https://research.facebook.com/research-awards/ethics-in-ai-research-initiative-for-the-asia-pacific-request-for-proposals/#award-recipients

3. Facebook announces award recipients of the Ethics in AI Research Initiative for the Asia Pacific. URL: https://research.facebook.com/blog/2020/06/facebook-announces-award-recipients-of-the-ethics-in-ai-research-initiative-for-the-asia-pacific/

4. Generative AI Has an Intellectual Property Problem. URL: https://hbr.org/2023/04/generative-ai-has-an-intellectual-property-problem

5. GitHub faces lawsuit over Copilot AI coding assistant. URL: https://www.infoworld.com/article/3679748/github-faces-lawsuit-over-copilot-coding-tool.html

6. Hikmah N. Digitalization of Islamic Law to Optimize the Existence of Islam in Millennial Generation. Al-Islam // Journal of Religion and Civilization. 2022. Vol. 1(1). Pp. 6–10.

7. URL: https://www.hbku.edu.qa/en/cis/staff/mohammed-ghaly

8. URL: https://www.ieai.sot.tum.de/

9. Isah Onuweh Jimoh Qur'an Addresses Science and Technology // International // Journal of Research and Innovation in Social Science (IJRISS). 2019. Vol. 45. Pp. 415–426.

10. ITU-UNESCO Regional Digital Inclusion Week: "Ensuring equity and inclusivity in all that we do: Data, Platforms and Policies". URL: https://www.itu.int

11. Muslim scholars are working to reconcile Islam and AI. URL: https://www.wired.co.uk/article/islamic-ai

12. Plagiarism cases growing at U of Manitoba as students increasingly turn to artificial intelligence. URL: https://www.cbc.ca/news/canada/manitoba/u-of-m-plagiarism-ai-chatgpt-1.6954819

13. Shaikh Mohd Saifuddeen bin Shaikh Mohd Salleh Quranic motivation for using information and communication technology (ict) in daawah // Centre of Quranic Research International Journal. 2012. Vol. 2, No. 1. Pp. 63–72.

14. The Holy Qur'an Arabic text and English translation. Translated by MaulawI Sher AlI. Tilford (UK): Islam international publications LTD, 1989. 1028 p.

15. These are the countries where Chat GPT is currently banned. URL: https://www.digitaltrends.com/computing/these-countries-chatgpt-banned/

16. Towards a common Artificial Intelligence strategy for Arab States: Digital Inclusion Week 2021. URL: https://www.unesco.org/en/articles/towards-common-artificial-intelligence-strategy-arab-states-digital-inclusion-week-2021

17. Yasmansyah Lainah, Zulfani Sesmiarni. Science and technology in the quran education method // Jurnal ipteks terapan. Research of Applied Science and Education. 2021. Vol. 15. Pp. 466–473.

18. Gromova E. A., Petrenko S. A. Quantum Law: The Beginning // Journal of Digital Technologies and Law. 2023. Vol. 1(1). Pp. 62–88.

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ МЕЖДУНАРОДНО-ПРАВОВЫХ ОТНОШЕНИЙ

DIGITAL TECHNOLOGIES IN THE SYSTEM OF INTERNATIONAL-LEGAL RELATIONS

С. А. Борш,
специалист,
Приднестровский государственный университет
имени Т. Г. Шевченко
Ю. А. Скубий,
старший преподаватель,
Приднестровский государственный университета
имени Т. Г. Шевченко

ПРИМЕНЕНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В МЕЖДУНАРОДНОМ ПРАВЕ

Аннотация. В статье представлена информация о влиянии цифровых технологий на международное право и международные отношения. Описываются секторы экономики, которые могут претерпеть изменения в связи с цифровизацией. Раскрывается влияние Интернета и на нормы международного права в целом.

Ключевые слова: оцифровка, цифровое право, информационное право, интернет-право, закон онлайн-сетей, закон киберпространства

APPLICATION OF DIGITAL TECHNOLOGIES IN INTERNATIONAL LAW

Abstract. The article provides information on the impact of digital technologies on international law and international relations. It describes the sectors of the economy that may undergo changes due to digitalization. The influence of the Internet and social media platforms on the norms of international law is revealed.

Keywords: digitization, digital law, information law, Internet law, the law of online networks, the law of cyberspace

Цифровая экономика и современное общество, все больше ориентированные на компьютеризацию, неизбежно требуют появления «цифрового права». Его роль заключается в регулировании не только общественных отношений в виртуальной среде, но и в отношении цифровых товаров в форме данных и информации [1].

Специфика цифровой сферы означает, что классические правовые нормы и институты не могут быть автоматически применены к ней [2]. Более того, в настоящее время нет четкого ответа относительно конкретного способа адаптации ранее существовавших правовых норм к виртуальной среде.

При этом не следует ставить знак равенства между очевидной цифровизацией права все более присутствующей в последние годы во всех его отраслях, и цифровым правом, как возможной новой отраслью права. Поэтому мы считаем, что существенная роль в определении и исследовании сферы так называемого цифрового права будет в ближайшие годы принадлежать как академическому сообществу, так и судебной практике, которая, безусловно, будет призвана задуматься о том, как классические правовые нормы найдут свое место и адаптируются (или нет!) к цифровой среде.

Законодателю со своей стороны следует учитывать этот гибрид физического и цифрового, образующий системную целостность, созданную социальными отношениями. Поэтому недостаточно понять, как цифровые технологии влияют на общественные отношения, соответственно, на желания и стремления людей, мы также должны установить, как цифровые технологии будут развиваться и функционировать в рамках правовой системы.

Интернет-право

В США и большинстве стран Европейского союза интернет-право уже стало учебной дисциплиной. Первые упоминания появились еще в 1991 году, но наиболее важные нормативные акты появились значительно позже. Право стало доминировать в новой сфере общественных отношений, которая формировалась в интернет-пространстве вместе с развитием самого этого пространства.

Поэтому наиболее значимые научные публикации по общим вопросам, связанным с проблемой цифровизации, относятся к 1990-м годам, при этом активно интегрировались различные аспекты общественных отношений и отраслей права от физической среды к цифровой (например, интеллектуальная собственность, телекоммуникации, право на неприкосновенность частной жизни, киберпреступность и регулирование медиаконтента).

Многие исследователи считали, что цифровизация общественных отношений неизбежно затронет все отрасли права, но в первую очередь коснется институтов контракта, недобросовестной конкуренции и конституционного права [5]. Другие утверждают, что интернет-право будет краткосрочным продуктом, созданным технологическими инновациями, и неизбежно будет интегрировано в существующие правовые институты и отрасли права [4].

С другой стороны, одни авторы рассматривают интернет-право как новую отрасль права, другие называют его отраслью законодательства. Наконец, интернет-право также можно считать особым типом сложного правового института. С доктринальной точки зрения единодушно признано, что интернет-право заслуживает отдельного места в современном правовом ландшафте.

В настоящее время мы понимаем, что интернет-право, без сомнения, является новой отраслью юридической науки, которая, в свою очередь, породила новый ряд понятий, таких как право онлайн-сетей, право информации, цифровое право, право киберпространства. Практически интернет-право представляет собой совокупность правовых норм, призванных регулировать правоотношения, возникающие в связи с Интернетом. В рамках такого методологического подхода данный свод правил должен быть направлен на прямое или косвенное решение системных

проблем, порождаемых интернет-правом. С одной стороны, этот свод правил можно рассматривать как единое целое, а с другой стороны, не существует самостоятельного метода регулирования интернет-права, хотя эти онлайн-отношения явно отличаются от других общественных отношений. Особенность интернет-права состоит в специфике решения проблем, связанных с коллизией юрисдикций и коллизионным правом в виртуальном пространстве.

Хотя бесспорно, что родиной интернет-права являются США, в последние годы этот вопрос стал интенсивно беспокоить Европейский союз, который начал принимать законы во многих областях, таких как борьба с компьютерной преступностью, электронная коммерция, смарт-контракты, защита прав потребителей, авторское право, защита данных, банковское дело и т. д. Одной из последних инициатив Европейского Союза, связанных с областью интернет-права, является уже известный Регламент № 679 от 27 апреля 2016 г. о защите физических лиц при обработке персональных данных и о свободном перемещении таких данных, а также об отмене Директивы 95/46/ЕС (Общий регламент по защите данных – GDPR), а также Директива (ЕС) 2019/790 Европейского парламента и Совета от 17 апреля 2019 г. об авторском праве и смежных правах на едином цифровом рынке и вносит поправки в Директивы 96/9/ЕС и 2001/29/ЕС. Когда мы обсуждаем Директиву об авторском праве 2019/790, очевидные противоречия между корпорациями, «владеющими» Интернетом (иногда называемыми GAFA: Google, Amazon, Facebook*, Apple), или активистами, борющимися за «свободный» Интернет (например, Electronic Frontier Foundation), с одной стороны, и правообладателями или создателями контента, с другой, становятся очевидными.

Новый пакет предложений по нормативным актам на уровне Евросоюза в сфере цифровых услуг включает Положение о состязательных и справедливых рынках в цифровом секторе (Законодательный акт о цифровых рынках) и Положение о едином рынке цифровых услуг (Законодательный акт). Закон о цифровых услугах) и поправки к Директиве 2000/31/CE, которые уже были приняты Европейским парламентом в июле 2022 года и будут приняты в ближайшем будущем Советом Европейского союза.

Основными целями, которые рассматривал европейский законодатель при разработке этих двух предложенных нормативных актов, было создание более безопасного цифрового пространства, в котором будут защищены основные права всех пользователей цифровых услуг, а также создание условий справедливой конкуренции для стимулирования инноваций, роста и конкурентоспособности как на едином европейском рынке, так и во всем мире.

Цифровые услуги включают в себя большую категорию онлайн-услуг: от простых веб-сайтов до услуг интернет-инфраструктуры и онлайн-платформ.

Правила, указанные в Законе о цифровых услугах (DSA), в первую очередь касаются посредников и онлайн-платформ. Например, онлайн-торговые площадки, социальные сети, платформы для обмена контентом, магазины приложений и онлайн-платформы для путешествий и размещения.

Закон о цифровых рынках (DMA) включает правила, регулирующие онлайн-платформы-привратники. Платформы Gatekeeper – это цифровые платформы,

играющие системную роль на внутреннем рынке, которые выступают посредниками между бизнес-средой и потребителями важных цифровых услуг. Некоторые из этих услуг также покрываются DSA, но по другим причинам и с разными типами условий.

Быстрое и масштабное развитие цифровых услуг лежит в основе цифровых изменений, влияющих на нашу жизнь. Существует множество новых способов общения, покупки или доступа к информации в Интернете, которые постоянно развиваются. Нам необходимо обеспечить, чтобы европейское законодательство развивалось вместе с ними.

Онлайн-платформы создали значительные преимущества для потребителей, а внедренные ими инновации помогли внутреннему рынку Европейского союза стать более эффективным. Они также способствовали трансграничной торговле внутри и за пределами Европейского союза. Таким образом, для европейской деловой среды появились новые возможности, способствующие ее расширению и доступу на новые рынки.

Хотя существует широкий консенсус относительно преимуществ этой трансформации, возникающие проблемы имеют многочисленные последствия для нашего общества и экономики [3]. Основной проблемой является незаконная торговля и обмен товарами, услугами и контентом в Интернете. Онлайн-сервисы также используются манипулятивными алгоритмическими системами для усиления распространения дезинформации и других вредоносных целей. Эти новые проблемы и подход платформ к ним оказывают существенное влияние на фундаментальные права в онлайн-среде.

Несмотря на целый ряд отраслевых мер на уровне Европейского союза, все еще существуют значительные пробелы и разнообразные правовые задачи, которые необходимо решить.

Ускоренная цифровизация общества и экономики создала ситуацию, когда несколько крупных платформ контролируют важные экосистемы цифровой экономики. Они стали своего рода стражами цифровых рынков, наделенными полномочиями действовать как своего рода частные законодатели. Эти правила иногда приводят к созданию несправедливых условий для различных форм бизнеса, использующих эти платформы, и ограничению возможностей для потребителей.

В свете этих событий Европе необходима современная правовая база, которая обеспечит безопасность онлайн-пользователей, поставит защиту основных прав на первый план и поддержит справедливую и открытую среду онлайн-платформы.

После принятия Советом Европейского союза и DMA, и DSA будут подписаны президентами обоих институтов и опубликованы в Официальном журнале. Оба закона вступят в силу через 20 дней после их публикации в Официальном журнале.

DSA будет применяться напрямую на всей территории Европейского союза через пятнадцать месяцев или с 1 января 2024 года, в зависимости от того, что наступит позже, после вступления в силу. Что касается обязательств для очень крупных онлайн-платформ и поисковых систем, DSA начнет применяться с более ранней даты, то есть через четыре месяца после их назначения.

После вступления в силу DMA оно начнет применяться через шесть месяцев. Назначенным привратникам будет предоставлено максимум шесть месяцев с момента принятия Комиссией решения о назначении, чтобы обеспечить соблюдение обязательств, изложенных в DMA.

Эффекты, которые окажет этот нормативный пакет, сейчас трудно оценить!

А на уровне ООН вопрос цифровизации стоит на повестке дня работы. Так, по инициативе Генерального секретаря ООН в целях предоставления рекомендаций о том, как международное сообщество могло бы сотрудничать в целях оптимизации использования цифровых технологий и снижения рисков, в 2018 году была создана Группа высокого уровня по цифровому сотрудничеству. В июне 2019 года он опубликовал доклад «Эпоха цифровой взаимозависимости» и вместе с ним ряд рекомендаций по улучшению цифрового сотрудничества. Среди таких рекомендаций следует отметить:

– к 2030 году каждый взрослый должен иметь доступ к цифровым сетям, а также к цифровым финансовым и медицинским услугам;

– создание широкой платформы для обмена цифровыми общественными благами с соблюдением конфиденциальности;

– призыв к частному сектору, гражданскому обществу, национальным правительствам, транснациональным банкам и ООН принять конкретную политику в целях поддержки полного охвата цифровыми технологиями и цифрового равенства для женщин и традиционно маргинализированных групп;

– разработка набора матриц для включения цифровых технологий;

– создание региональных и глобальных цифровых справочных служб, чтобы помочь правительствам, гражданскому обществу и частному сектору разобраться в цифровых проблемах и развить потенциал для руководства социальным сотрудничеством;

– с учетом того, что права человека полностью применяются в цифровом мире, Генеральному секретарю ООН необходимо будет создать общеведомственный реестр того, как существующие международные соглашения и стандарты в области прав человека применяются к новым и возникающим цифровым технологиям;

– перед лицом растущих угроз правам и безопасности человека, в том числе детей, средствам массовой информации необходимо будет сотрудничать с правительствами, международными и местными организациями гражданского общества и экспертами со всего мира, чтобы полностью понять и отреагировать на обеспокоенность по поводу существующих или потенциальных нарушений прав человека;

– автономные интеллектуальные системы должны быть спроектированы таким образом, чтобы они позволяли объяснять их решения и чтобы люди могли нести ответственность за то, как они используются;

– международные организации, такие как Всемирный банк и ООН, должны усилить исследования и содействовать действиям по устранению барьеров, с которыми сталкиваются женщины и маргинализированные группы в плане цифровой интеграции и цифрового равенства.

В ответ на отчет более 100 государств-членов и организаций представили отзывы и вызвались возглавить или принять участие в обсуждениях по одной или нескольким рекомендациям группы.

11 июня 2020 года Генеральный секретарь Организации Объединенных Наций Антониу Гутерриш представил международному сообществу ряд рекомендуемых действий, призванных помочь обеспечить связь, уважение и защиту всех людей в эпоху цифровых технологий. Дорожная карта Генерального секретаря по цифровому сотрудничеству является результатом многолетних глобальных усилий многих заинтересованных сторон по решению ряда проблем, связанных с Интернетом, искусственным интеллектом и другими цифровыми технологиями.

В дорожной карте представлены рекомендации Генерального секретаря ООН относительно конкретных действий различных заинтересованных сторон по укреплению глобального цифрового сотрудничества в следующих областях:

– достижение всеобщего подключения к 2030 году – доступ каждого к безопасному Интернету;

– продвижение цифровых общественных благ для создания более справедливого мира;

– обеспечение охвата цифровыми технологиями для всех, включая наиболее уязвимые группы населения – малообеспеченным группам необходим равный доступ к цифровым инструментам для ускорения развития;

– наращивание цифрового потенциала – развитие навыков и обучение необходимы во всем мире;

– обеспечение защиты прав человека в эпоху цифровых технологий – права человека применяются как онлайн, так и офлайн;

– поддержка глобального сотрудничества в области надежного, основанного на правах человека, безопасного, устойчивого и способствующего миру искусственного интеллекта;

– содействие цифровому доверию и безопасности – призыв к глобальному диалогу для достижения Целей устойчивого развития;

– создание более эффективной архитектуры цифрового сотрудничества, сделав цифровое управление приоритетом на уровне ООН.

Дорожная карта Генерального секретаря ООН основана на рекомендациях Группы высокого уровня по цифровому сотрудничеству и вкладе государств-членов, частного сектора, гражданского общества, технического сообщества и других заинтересованных групп.

Однако в ближайшее время предстоит решить определенные проблемы, которые на первый взгляд кажутся труднорегулируемыми.

Прежде всего, речь идет о праве на частную жизнь, проявляющемся в виртуальном пространстве через право любого человека на подключение. Но эта проблема, хотя она и кажется простой, порождает значительные проблемы, порожденные способностью основных участников онлайн-среды (Google, Amazon и т. д.) хранить данные, использовать их и даже продавать различным компаниям, стремящимся продавать товары в Интернете. По сути, мы имеем дело с продажей нашего онлайн-поведения, которое становится коммерческим товаром!

Во-вторых, существует проблема кибербезопасности, которая требует международного сотрудничества. Мы имеем дело с проблемой искусственного интеллекта, точнее с проблемой порождаемых им эффектов.

Все эти проблемы могут быть решены только на основе консенсуса всех вовлеченных стран. С одной стороны, это можно сделать на законодательном уровне, приняв новые нормативные акты, а с другой – создав цифровые диалоговые площадки, связанные с отдельными составляющими «жизни» онлайн: бизнес-средой, научным сообществом, гражданским обществом и т. д.

Наконец, возможно, самой важной проблемой является цифровое неравенство. Большая часть населения мира не имеет доступа к Интернету. Это порождающий источник неравенства, который приводит к серьезному социальному неравенству, что очень затрудняет развитие в странах, которые не имеют возможности предоставить доступ к Интернету населению.

Секторы экономики, которые претерпят изменения в связи с цифровизацией

А. Использование криптовалют

В нынешних условиях использование криптовалют в качестве альтернативы существующим валютам кажется более интересным, чем раньше. В основном это связано с тем, что меры государственной поддержки направлены на ослабление классических валют. Нынешняя тенденция к реализации огромных пакетов государственной поддержки, усугубленная недавним кризисом, вызванным вирусом SARS-CoV-2, без попыток минимального понимания контекста, породившего кризис, а также тенденция сохранения существующей экономики для дальнейшего развития. Как бы долго ни считали это необходимым, они только усиливают беспокойство по поводу стабильности валют.

Маловероятно, что виртуальные валюты станут платежным средством, которое позволит какое-либо правовое регулирование, поскольку в настоящее время очень сложно запретить обмен виртуальных валют на национальную валюту.

Более того, криптовалюты также могут выиграть от возможного снижения эксплуатационных расходов сети, что сделает их майнинг менее дорогостоящим.

В этом контексте очень важно, чтобы система криптовалют обеспечила большую прозрачность. Важным компонентом с этой точки зрения является эффективное регулирование рынка криптовалют, тем более что эти платежные инструменты могут легко использоваться в мошеннических целях, например, для отмывания денег.

Однако, поскольку мы все еще находимся на ранней стадии развития этих типов финансовых инструментов, есть возможности для лучшего и более эффективного использования технологического прогресса в этой области.

Б. Замена традиционных корпораций посредством цифровизации

Бывают случаи, когда технологические инновации способны разрушить отрасль, и Tesla является доказательством того, что это может произойти в автомобильной промышленности. В то же время маловероятно, что в автомобильной отрасли будут заменены все традиционные операторы. Скорее, то, что наблюдается некоторое время в фармацевтической отрасли, представляется характерным

для того, что будет происходить в будущем и в других сферах, соответственно мы станем свидетелями адаптации к рыночным требованиям уже существующих игроков, в том числе посредством сотрудничества (в едином так или иначе) со стартапами, которые могут быть более инновационными, но которым, в свою очередь, необходим рыночный опыт уже существующих компаний, чтобы привлечь потенциальных новых покупателей или возможные источники дополнительного финансирования.

B. Последствия кризиса Covid-19 для цифровизации

Понятно, что одним из главных последствий недавнего кризиса Covid-19 (еще не полностью завершенного!) стал отказ от некоторых инвестиций, которые, вероятно, можно было бы сделать в цифровизацию. С другой стороны, этот кризис ускорил адаптацию рынка труда к элементу, который, казалось, находится в далеком будущем, а именно к онлайн-работе. Однако с постепенным выходом из кризиса большинство корпораций уже не будут полностью отказываться от преимуществ онлайн-работы, а захотят внедрить новые процедуры, чтобы сделать этот сектор более эффективным.

Увеличение мощности обработки данных, возможное за счет оцифровки, могло бы повысить эффективность курсов для достижения определенного результата. Можно разработать онлайн-программы для индивидуального измерения навыков. Это можно использовать для детального обучения составлению контрактов. Переход от традиционного обучения, сосредоточенного на теории и судебной практике, к более или менее сложному составлению документов представляется более целесообразным, поскольку большинство практикующих юристов действительно занимаются составлением документов, и лишь часть меньших из них готовят дела строго от точки зрения теории.

В заключение следует отметить, что роль технологий можно расширить практически в любой области, принося добавленную стоимость и повышая эффективность. В рамках этого процесса наименее сложные виды деятельности имеют наибольшие шансы быть оцифрованными.

В этом процессе юристы не смогут быть заменены, а будут выступать участниками и даже менеджерами изменений, придавая им содержание. Постепенные изменения иногда могут стать ускоренными. Красноречивым примером в этом смысле является возможность проводить встречи онлайн, элемент, который помогает, когда эти встречи – независимо от их характера - больше не могут проводиться физически, как это произошло в контексте кризиса Covid-19.

---

* Meta и принадлежащие ей Facebook и Instagram признаны экстремистскими, их деятельность запрещена на территории Российской Федерации.

Список литературы

1. Гольдман Э., Преподавание киберправа // Юридический журнал Университета Сент-Луиса. 2008. № 52(3). С. 749-764.

2. Эдвардс Л., Вельде К. Закон и Интернет. Bloomsbury Publishing, 2009.

3. Ярутин Я. К., Гуляева Е.Е. Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. 725-751.

4. Kerr O. S. The Problem of Perspective in Internet Law // Georgetown Law Journal. 2003. Vol. 91. Pp. 357-405.

5. Sommer, Joseph H. Against Cyberlaw // Berkley Technology Law Journal. 2000. Vol. 15, Iss. 3. Pp. 1145-1232.

А. С. Бурнасов,
кандидат исторических наук, доцент,
Уральский федеральный университет
имени Первого президента Б. Н. Ельцина

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА НА БЛИЖНЕМ ВОСТОКЕ

Аннотация. В статье обращено внимание на роль и влияние цифровых технологий в обеспечении международного сотрудничества на Ближнем Востоке. В современном глобализированном мире, где электронные коммуникации и информационные технологии проникают в различные сферы жизни, использование цифровых технологий становится все более важным в контексте укрепления международных, экономических, социальных, правовых и культурных связей между странами Ближнего Востока. Исследование основывается на анализе последних исследовательских результатов, научных статей, статистических данных и официальных документов, связанных с применением цифровых технологий в обеспечении международного сотрудничества на Ближнем Востоке. Оно также включает анализ подходов к составлению базы данных организаций на Ближнем Востоке для развития сотрудничества. Работа выполнена в рамках Научного центра компетенции УрФУ «Диаспоральные сообщества в условиях трансформации глобальной политической системы и мирохозяйственных связей». Полученные результаты могут быть полезными для международных организаций, правительственных структур, бизнес-сектора и академического сообщества, заинтересованных в развитии международного сотрудничества на Ближнем Востоке с использованием цифровых технологий.

Ключевые слова: право, цифровые технологии, Ближний Восток, база данных, международное сотрудничество, партнерство, развитие

DIGITAL TECHNOLOGIES FOR INTERNATIONAL COOPERATION IN THE MIDDLE EAST

Abstract. This article draws attention to the role and impact of digital technologies in facilitating international cooperation in the Middle East. In today's globalized world, where electronic communications and information technology permeate various spheres of life, the use of digital technologies is becoming increasingly important in the context

of strengthening international, economic, social, legal and cultural ties among Middle Eastern countries. The study is based on the analysis of recent research findings, academic articles, statistical data and official documents related to the application of digital technologies in promoting international cooperation in the Middle East. It also includes an analysis of approaches to compiling a database of organizations in the Middle East to promote cooperation. The work was carried out within the framework of the UrFU Scientific Center of Competence «Diaspora communities in the conditions of transformation of the global political system and world economic relations». The results obtained can be useful for international organizations, governmental structures, business sector and academic community interested in the development of international cooperation in the Middle East using digital technologies.

Keywords: law, digital technology, Middle East, database, international cooperation, partnership, development

В XXI веке цифровые технологии стали ключевым фактором в обеспечении и укреплении международного сотрудничества на Ближнем Востоке. С развитием информационных технологий и электронных коммуникаций возможности для установления и поддержания контактов между различными странами и регионами значительно расширились. Российские зарубежные соотечественники на Ближнем Востоке успешно использовали эти технологии, создавая базу для организации, способствующей развитию сотрудничества.

Информационная среда стала надежной основой для формирования и развития сети контактов, объединяющей российских граждан, проживающих за пределами России, и способствующей активному взаимодействию между ними и российскими организациями, предприятиями и соотечественниками.

В данной статье мы рассмотрим влияние цифровых технологий на обеспечение международного сотрудничества на Ближнем Востоке, сферы их успешного применения, а также пример создания базы данных Организации российских зарубежных соотечественников на Ближнем Востоке в XXI веке. Мы также проанализируем социальные, экономические и культурные аспекты, связанные с внедрением цифровых технологий, и проследим их влияние на укрепление сотрудничества в регионе.

Цифровые технологии имеют огромный потенциал для укрепления и улучшения международного сотрудничества между неправительственными организациями. Технологии предоставляют широкий спектр инструментов и возможностей, которые помогают организациям эффективно взаимодействовать, обмениваться информацией и координировать свою деятельность на международном уровне:

– во-первых информационные технологии обеспечивают глобальную связность. Цифровые технологии позволяют неправительственным организациям оперативно связываться с партнерами и участниками в разных странах. Они могут использовать электронную почту, видеоконференции, сетевые платформы и социальные медиа для обмена информацией, проведения совместных встреч и координации своих усилий;

– во-вторых технологии обеспечивают доступ к информации. Цифровые технологии обеспечивают доступ к обширным базам данных, исследовательским материалам, отчетам и другим источникам информации, что помогает неправительственным организациям быть информированными и обосновывать свои решения на основе фактических данных. Кроме того, они могут использовать онлайн-платформы для обмена лучшими практиками, обучения и роста профессиональных навыков;

– в-третьих, информационные технологии формируют мобильность и гибкость процессов сотрудничества. Цифровые технологии позволяют неправительственным организациям работать гибко и мобильно. Они могут использовать мобильные приложения и облачные сервисы для управления проектами, волонтерскими программами и финансами в режиме реального времени, даже на удаленных территориях. Это повышает эффективность и оперативность их работы;

– в-четвертых поддерживают социальное взаимодействие. Цифровые технологии способствуют укреплению социального взаимодействия и солидарности между неправительственными организациями. Их участники могут активно обмениваться идеями, опытом, ресурсами и поддержкой через онлайн-форумы, группы в социальных сетях и цифровые платформы, укрепляя тем самым сообщество и повышая влияние своих усилий. Таким образом, цифровые технологии играют важную роль в обеспечении международного сотрудничества неправительственных организаций, расширяя их возможности в коммуникации, информационном доступе, мобильности и социальном взаимодействии. Это открывает новые перспективы для реализации совместных проектов, достижения общих целей и создания более сильного и эффективного глобального сообщества неправительственных организаций.

Одним из важнейших инструментов информационных технологий в реализации международного сотрудничества является составление баз данных (далее – БД). Базы данных позволяют идентифицировать и связывать различные организации, группы или индивидуальных участников международного сотрудничества. Это помогает установить контакт и обменяться информацией между участниками, способствуя эффективному взаимодействию и сотрудничеству. Кроме того, базы данных позволяют хранить, организовывать и управлять информацией о проектах, контактах, ресурсах и других аспектах международного сотрудничества. Это облегчает доступ к необходимым данным, упрощает поиск и обмен информацией между участниками. Также базы данных являются важным инструментом для анализа и планирования сотрудничества. Путем анализа данных можно выявить тренды, потребности и возможности для дальнейшего развития сотрудничества. Это позволяет принимать информированные решения, разрабатывать стратегии и планы действий. БД позволяют отслеживать ход выполнения проектов и мониторить их результаты. Это позволяет проводить оценку и анализ эффективности сотрудничества, выявлять успешные практики и области для улучшения. Мониторинг и оценка помогают обеспечить прозрачность, отчетность и улучшение в долгосрочной перспективе. С помощью базы данных облегчают поиск новых партнеров, ресурсов и возможностей для расширения международного сотрудничества.

Записи и контакты в базах данных могут быть использованы для установления новых связей, инициирования проектов и развития новых форм сотрудничества. В целом, составление БД по международному сотрудничеству способствует более эффективному и организованному взаимодействию между участниками, улучшает планирование и мониторинг проектов, а также облегчает поиск новых возможностей для развития сотрудничества.

Перед составлением базы данных Организации российских зарубежных соотечественников на Ближнем Востоке в XXI веке были поставлены следующие задачи: позволять создать распределенную сеть контактов между российскими соотечественниками и предоставляет возможность обмена профессиональным опытом, знаниями и возможностями. Это может способствовать развитию бизнеса, научного и культурного сотрудничества и другим формам коллективного действия; должна содержать информацию о мероприятиях, проектах, новостях, ресурсах и возможностях, связанных с российскими соотечественниками на Ближнем Востоке. Это помогает участникам сообщества быть в курсе событий и использовать доступные им ресурсы; должна была помочь объединить российских соотечественников на Ближнем Востоке и создать единое сообщество. Это способствует установлению связей, обмену информацией и поддержке друг друга. В целом база данных способствует взаимодействию, поддержке и развитию российской диаспоры на Ближнем Востоке в XXI веке.

Стоит отметить вызовы в сфере международного права при составлении базы данных международного сотрудничества неправительственных организаций:

– во-первых, это защита интеллектуальной собственности в странах присутствия некоммерческих организаций;

– во-вторых, это вопросы защиты данных и приватность. При использовании цифровых технологий возникают вопросы о сборе, хранении и передаче данных, а также о защите личной информации. Международное право должно определить нормы и стандарты, регулирующие защиту данных и приватность, чтобы обеспечить соответствие неправительственных организаций международным стандартам;

– в-третьих, учет границ и суверенита страны. Использование цифровых технологий также поднимает вопросы о юрисдикции, границах и суверенитете в киберпространстве. Международное право должно разработать нормы и принципы, определяющие права и обязанности государств и неправительственных организаций в использовании цифровых технологий, учитывая вопросы суверенитета и защиты интересов государства;

– в-четвертых, поддержка международной стандартизации. Для эффективного использования цифровых технологий в международном сотрудничестве неправительственных организаций необходимо развивать сотрудничество и устанавливать стандарты и нормы, чтобы обеспечить совместимость и взаимодействие между различными системами и платформами. Международное право может способствовать координации усилий и созданию общих правил, например, в области обмена информацией и стандартов сбора, хранения и обработки баз данных.

При составлении базы данных Организации российских зарубежных соотечественников на Ближнем Востоке в XXI веке, использовались следующие методы: во-первых, опросы и анкетирование, были разработаны характеристики базы данных, которые содержат необходимую информацию, и был организован процесс сбора данных от части организаций российских соотечественников; во-вторых, при составлении также были использованы доступные веб-ресурсы, социальные сети, базы данных, профессиональные платформы или специализированные сайты, где эти организации были зарегистрированы или активны; в-третьих, были выстроены партнерские связи с рядом партнеров в регионе: консульствами, внешнеторговыми палатами, представительствами РЦНК или другими ассоциациями. При этом важно было учитывать конфиденциальность и соблюдать применимые правила и законы о защите данных при использовании любых методов сбора информации.

Основа БД – данные, содержащиеся в открытых источниках, относящихся к базе Организации российских зарубежных соотечественников на Ближнем Востоке в XXI в. После анализа содержания в открытых источниках (сеть Интернет) была структурирована имеющаяся в них информация, разработана структура БД, алгоритм внесения данных и осуществлен ввод данных. БД состоит из информации о 105 организациях российских зарубежных соотечественников на Ближнем Востоке в XXI в. Каждая единица БД включает 21 поле с характеристиками данных документов. БД представляет собой структурированный массив унифицированных текстовых, числовых и категориальных (логических) данных, обеспечивает поиск и оперативное проведение анализа для углубленных исследований; может подлежать ежегодному обновлению информации. Цель создания БД – создать формализованный аналитический инструментарий для проведения исследований экспертных исследований среди российских зарубежных соотечественников на Ближнем Востоке в XXI в. и анализа. БД предназначается для исследователей в области российских зарубежных соотечественников и специалистов управленческого звена российских регионов и федерального уровня государственной власти в области развития международного сотрудничества с организациями российских зарубежных соотечественников на Ближнем Востоке в XXI в. Результаты обработки данных могут быть использованы в составе систем поддержки принятия решений о выборе наиболее привлекательных партнеров среди организаций российских соотечественников. Информация, содержащаяся в БД, также будет полезной для выявления лидеров среди организаций российских зарубежных соотечественников на Ближнем Востоке в XXI в.

Структура базы данных и принципы применения. Принадлежность к целым числам для значения по столбцу указана явным образом для каждого параметра. В обратном случае параметр может принимать значение по непрерывной области значений. Поля, идентифицирующие локацию записи в базе данных. Формальные характеристики проводимых мероприятий организаций российских зарубежных соотечественников: порядковый номер – числовой тип, целочисленное, ключевой элемент, заполнение обязательно. Заполнение осуществлялось на основе порядкового номера; страна – текстовый тип, заполнение обязательно, заполняется

в соответствии со страной месторасположения организаций российских зарубежных соотечественников на Ближнем Востоке в XXI в.; наименование организации соотечественников – текстовый тип, заполняется в соответствии с официальным названием организациями российских зарубежных соотечественников на Ближнем Востоке в XXI в. Цель деятельности – текстовый тип, заполняется в соответствии с официальной целью организациями российских зарубежных соотечественников на Ближнем Востоке в XXI в. Пример: является официальным просветительским учреждением, работающим в Египте в области международных культурных и научных связей; краткое описание деятельности – текстовый тип, заполняется в соответствии с реализуемыми проектами организации на основе открытой информации об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; количество участников – текстовый тип, заполняется в соответствии с реализуемыми проектами организации на основе открытой информации об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; формальные характеристики проводимых мероприятий организаций российских зарубежных соотечественников; количество мероприятий, проводимых в год – текстовый тип, заполняется в соответствии с количеством мероприятий организации на основе информации в официальном аккаунте об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; источники поддержки – текстовый тип, заполняется в соответствии с анализом информации с официальных аккаунтов о партнерах мероприятий, реализуемых проектами организации на основе открытой информации об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; примерный охват – количество участников мероприятий – текстовый тип, заполняется в соответствии с анализом информации с официальных аккаунтов о количестве участников мероприятий, реализуемых проектами организации на основе открытой информации об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; Примерный охват (страны, может быть регион) – текстовый тип, заполняется в соответствии с анализом информации с официальных аккаунтов о странах в которых еще проходит мероприятие, реализуемое проектами организации на основе открытой информации об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; контакты организаций российских зарубежных соотечественников: руководитель ФИО – текстовый тип, заполняется в соответствии с информацией о руководителе организации на основе информации в официальном аккаунте об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; должность руководителя – текстовый тип, заполняется в соответствии с информацией о должности руководителя организации на основе информации в официальном аккаунте о организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; партнерские организации – текстовый тип, заполняется в соответствии с информацией о партнерских организациях на основе информации в официальном аккаунте о организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; адрес – текстовый тип, заполняется в соответствии с информацией об адресе организации на основе информации в офи-

циальном аккаунте об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; телефонный номер – текстовый тип, заполняется в соответствии с информацией о телефонном номере организации на основе информации в официальном аккаунте об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; электронная почта – текстовый тип, заполняется в соответствии с информацией об электронной почте организации на основе информации в официальном аккаунте о организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; сайт – текстовый тип, заполняется в соответствии с информацией о сайте организации на основе информации в официальном аккаунте о организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; год создания – текстовый тип, заполняется в соответствии с информацией о годе создания организации на основе информации в официальном аккаунте об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; страница в социальных сетях России – текстовый тип, заполняется в соответствии с информацией об аккаунте в социальных сетях организации на основе информации в официальном аккаунте о организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; страница в глобальных сетях – текстовый тип, заполняется в соответствии с информацией о странице в глобальных сетях организации на основе информации в официальном аккаунте об организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.; юридический статус (официальный и неофициальный) – текстовый тип, заполняется в соответствии с информацией о статусе сайта (официальный или неофициальный) организации на основе информации в официальном аккаунте о организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.

База данных Организации российских зарубежных соотечественников на Ближнем Востоке в XXI веке предоставляет ряд возможностей для использования: для поиска и установления контакта с другими российскими соотечественниками на Ближнем Востоке, при сетевом взаимодействии, обмене информацией или сотрудничестве в различных областях; содержать информацию о различных ресурсах и услугах, доступных для российских соотечественников. Вы можете использовать ее для поиска информации о консульских услугах, юридической помощи, образовательных возможностях, предпринимательских и культурных инициативах и других полезных ресурсах; служить площадкой для обмена опытом, знаниями и идеями между российскими соотечественниками на Ближнем Востоке; для поиска профессиональных контактов, обсуждения вопросов, связанных с вашей областью деятельности, и получения поддержки на основе опыта других участников сообщества; предоставлять информацию о мероприятиях, конференциях, вебинарах и других событиях, связанных с российской диаспорой на Ближнем Востоке; возможности использования базы данных позволяют российским соотечественникам на Ближнем Востоке активно взаимодействовать, обмениваться информацией и поддерживать связи между собой.

Список литературы

1. Актуальные проблемы Ближнего и Среднего Востока: сборник научных статей / отв. ред. А. М. Мустафабейли. М.: Дипломатическая академия МИД России, 2017. 169 с.

2. Андреев А. В. Россия на Ближнем Востоке за последние сто лет // Проблемы национальной стратегии. 2020. № 2(59). С. 232-238.

3. Ахмадеев А. Особенности использования данных из баз данных, являющихся объектом смежного права // Правовая защита интеллектуальной собственности: проблемы теории и практики: сборник материалов XI Международного юридического форума (IP Форум), Москва, 17–18 февраля 2023 года. Том 1. Москва: Московский государственный юридический университет имени О.Е. Кутафина (МГЮА), 2023. С. 120-122.

4. Ближний Восток в фокусе политической аналитики: сборник научных трудов: к 15-летию Центра ближневосточных исследований / Моск. гос. ин-т междунар. отношений (ун-т) Мин-ва иностр, дел Рос. Федерации, Ин-т междунар. исследований, Центр ближневосточных исследований. М.: ИМИ МГИМО, 2019. 548 с.

5. Попов В. Непростые дни Ближнего Востока. URL: https://russiancouncil.ru/analytics-and-comments/columns/middle-east/neprostye-dni-blizhnego-vostoka

6. Российские соотечественники в Африке и на Ближнем Востоке в условиях нестабильности // Портал «Русский мир». URL: https://russkiymir.ru/publications/223182/?sphrase_id=705964

7. Свидетельство о государственной регистрации базы данных № 2023620424 Российская Федерация. Организации российских зарубежных соотечественников на Ближнем Востоке в XXI в.: № 2022623667: заявл. 14.12.2022 : опубл. 01.02.2023 / А. С. Бурнасов, М. Р. Вафина, А. Д. Кирмель [и др.]; заявитель Федеральное государственное автономное образовательное учреждение высшего образования «Уральский федеральный университет имени первого Президента России Б. Н. Ельцина». EDN PFNAEE.

8. Тупицына Е. Г., Тупицын Н. В. К вопросу о базе данных как объекте интеллектуальных прав // Актуальные вопросы современной науки и образования: Сборник научных статей по материалам XVIII международной научно-практической конференции, Киров, 14-17 мая 2019 года. Киров: Московский финансово-юридический университет МФЮА, 2019. С. 317-323.

Н. Н. Гончарова,
кандидат юридических наук,
Казанский инновационный университет
имени В. Г. Тимирясова
Е. В. Дятлова,
старший преподаватель,
Казанский инновационный университет
имени В. Г. Тимирясова

РАЗВИТИЕ УГОЛОВНОГО ПРОЦЕССУАЛЬНОГО ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ПРОВЕДЕНИЯ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ С ИСПОЛЬЗОВАНИЕМ ВИДЕО-КОНФЕРЕНЦ-СВЯЗИ С ЛИЦАМИ, НАХОДЯЩИМИСЯ НА ТЕРРИТОРИИ ИНОСТРАННЫХ ГОСУДАРСТВ

Аннотация. Развитие уголовного процессуального законодательства Российской Федерации в исследуемом вопросе направлено на расширение возможностей проведения следственных действий, находящихся за пределами государственных границ государства, а также решение некоторых вопросов соблюдения принципа соблюдения прав участников уголовного процесса, учитывая стремительное развитие информационных технологий и внедрение их в работу следственных органов России.

Ключевые слова: государство, видео-конференц-связь, правовая помощь, внешние сношения, цифровые технологии, следственные действия, консульства

DEVELOPMENT OF CRIMINAL PROCEDURAL LEGISLATION IN THE FIELD OF INVESTIGATING ACTIONS USING VIDEO CONFERENCE COMMUNICATIONS WITH PERSONS IN THE TERRITORY OF FOREIGN STATES

Abstract. The development of the criminal procedural legislation of the Russian Federation in the issue under study is aimed at expanding the possibilities for conducting investigative actions that are outside the state borders of the state, as well as solving some issues of observing the principle of observing the rights of participants in the criminal process, given the rapid development of information technologies and their introduction into the work of the investigative bodies of Russia.

Keywords: state, video conferencing, legal assistance, external relations, digital technologies, investigative actions, consulates

Цифровые средства реализации государственных целей, задач и функций занимают центральное место среди актуальных вопросов научной и практической деятельности во всем мире. Современные технологии и программное обеспечение позволяют разрешить дилемму противоречия юрисдикционных вопросов и защиты прав человека, а также прежде всего участника предварительного расследования – свидетеля, потерпевшего и других [2, 4–6]. Возможности виртуального общения в интернет-пространстве многогранны и позволяют «сократить расстоя-

ние» между государством, государственным органом, должностным лицом и лицом, заинтересованным в исходе уголовного процесса.

Проблемы видео-конференц-связи при проведении допроса в рамках территории Российской Федерации рассматривались ранее такими авторами как П. А. Устинкин, в статье «Допрос с использованием систем видеоконференц-связи» [7. С. 39-43] были раскрыты перспективы развития норм УПК в рамках процедуры допроса, а Е. А. Артамонова исследовала производство видеодопроса в предварительном расследовании [1. С. 5-9].

В некоторых ранее опубликованных работах нами освещались возможные перспективы следственных действий на квазитерриториях Российской Федерации, в том числе в статье «Проблемы проведения уголовно-процессуальных действий с участием иностранных граждан на российской территории, а также в зданиях посольств и консульств России» [3].

А также рассматривались изменения декабря 2021 года (ФЗ № 501-ФЗ) в УПК РФ в части проведения допроса, очной ставки, опознания с использованием видео-конференц-связи и определен порядок проведения следственных действий, таких как направление поручения об организации участия лица в следственном действии, составление протокола и разъяснения прав участникам следственных действий, видеозапись и отправка документов, материалов, ордера адвоката следователю (ст. 189.1 УПК).

Отметим, что проведение конференцсвязи на территории посольств и консульств в перспективе также может осуществляться в соответствии с законодательством страны, на территории которой находится учреждение, а также на основе международных договоров и обычаев. В большинстве случаев, для проведения конференцсвязи необходимо получить разрешение и обеспечить присутствие соответствующих органов и служб безопасности посольства или консульства. Также могут потребоваться специальные технические средства и оборудование, которое может быть предоставлено посольством или консульством либо арендовано у сторонних организаций.

Действующее уголовное процессуальное право допускает, что лицо, обеспечивающее проведение следственных действий, при этом вполне способно совершить действия, не требующие специальных познаний и квалификации. Формализм и определенный порядок их выполнения позволяет выполнить организацию видео-конференц-связи даже сотрудникам дипломатического или консульского учреждения, учитывая в рамках актуальной политической обстановки сложность в реализации правовой помощи.

Без сомнения, требование о письменном поручении (ч. 2 ст. 189.1 УПК) должно быть безоговорочно выполнено и соблюдено.

Однако следует помнить, что в этом случае потребуется более тщательный подход к определению лиц, дающих показания, а также интерпретация этих данных. Частным случаем является допрос свидетеля, который находится на территории другой страны в ходе заседания суда. Так, законодательство не предусматривает дистанционного допроса лица, находящегося за пределами РФ, а лишь возможность его допроса на территории другой страны.

Необходимо отметить, что в январе 2023 года в Государственную Думу был внесен законопроект, который при его принятии позволит устранить перечисленные выше пробелы, а также официально узаконить применение видео-конференц-связи при следственных действиях на территории консульств, которые расположены на территориях других государств. Данным законопроектом предполагается изменение статей 453 и 456 УПК РФ.

А именно норму ч. 1 статьи 453 заменить на иную, которая гласит, что: «В исключительных случаях суд, прокурор, следователь, руководитель следственного органа, дознаватель по согласованию с Министерством иностранных дел Российской Федерации можгут внести запрос о проведении допроса, в том числе путем использования систем видео-конференц-связи, или о передаче процессуальных документов консульскими должностными лицами Российской Федерации в соответствии с международным договором Российской Федерации и требованиями настоящего Кодекса».

А норму ч. 2 статьи 456 УПК РФ изложить в следующем исполнении: «Запрос о вызове направляется в компетентные органы иностранного государства в порядке, установленном частью 3 статьи 453 настоящего Кодекса. В исключительных случаях запрос о вызове может быть направлен в том же порядке по согласованию с Министерством иностранных дел Российской Федерации консульским должностным лицам Российской Федерации в соответствии с международным договором Российской Федерации».

На данный момент рассмотрение законопроекта приостановлено в первом чтении. Его принятие отложено на неопределенное время.

Напомним, что процедура, закрепленная в УПК, направлена на соблюдение прав участников уголовного процесса, что является прямой функцией дипломатических учреждений.

Проблема реализации идеи использования систем видео-конференц-связи в рамках предварительного расследования до сих пор остается нерешенной в законодательстве, несмотря на его актуальность. Однако внедрение таких систем безусловно приведет к улучшению судебного процесса и повышению эффективности расследования. Оно позволит получать информацию о совершенных преступлениях быстрее, что, в свою очередь, способствует их более оперативному раскрытию.

Во-первых, следует отметить, что богатая география проживания соотечественников в том числе впечатляет, и иногда требуются длительное время и затраты для организации встречи свидетеля со следователем или для выезда следователя к месту его нахождения и постоянного проживания. Введение систем видео-конференц-связи позволит значительно сократить эти затраты и ускорить процесс сбора доказательств, что положительно скажется на сроках проведения уголовного процесса.

Во-вторых, для того чтобы повысить защиту информации и, эффективное взаимодействие между участниками процесса, необходимо учитывать такие технические аспекты, как качество связи, надежность связи. Возможные трудности с вывозом и неудобства при транспортировке часто отпугивают потенциальных

свидетелей от дачи более подробных показаний. Но при использовании системы видео-конференц-связи свидетели могут чувствовать себя свободнее и защищеннее.

В-третьих, видеозапись может быть использована в качестве дополнительного доказательства в ходе судебного разбирательства, что помогает более объективно рассмотреть дело.

В-четвертых, регулирование использования систем видео-конференц-связи приблизит наши национальные законы к законам других стран и возможно, приведет к универсальному подходу к проведению таких процедур. Это однозначно приведет к дополнению существующих двусторонних международных договоров о правовой помощи как минимум, к развитию универсального международного права как максимум, при благоприятном стечении обстоятельств.

В заключение отметим, что это важный шаг по модернизации правоохранительной системы и обеспечению справедливости при расследовании уголовных дел. Эти меры позволяют значительно сократить временные и материальные затраты, повысить эффективность расследований и обеспечить быстрое раскрытие преступлений. Но для того, чтобы обеспечить безопасность и надежность, необходимо тщательно сформулировать технические и организационные аспекты внедрения таких систем.

Список литературы

1. Артамонова Е. А. Размышления о производстве видео допроса в ходе предварительного расследования. URL: https://cyberleninka.ru/article/n/razmyshleniya-o-proizvodstve-videodoprosa-v-hode-predvaritelnogo-rassledovaniya/viewer

2. Асли М. Р. Цифровые тренды криминологии и уголовного правосудия XXI века // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 235-250. EDN ZMIRLT

3. Гончарова Н. Н., Латыпова Э. Ю., Гончаров Н. А. Проблемы проведения уголовно-процессуальных действий с участием иностранных граждан, на российской территории, а также в зданиях посольств и консульств России // Пробелы в российском законодательстве. 2021. Т. 14, № 4. С. 366-372.

4. Дмитриева А. А., Пастухов П. С. Концепция электронного доказательства в уголовном судопроизводстве // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 270-295. EDN SGAOKS.

5. Рэн Й. Люди-переводчики в виртуальных судах: обзор дистанционных технологических решений в Австралии // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 712-724. EDN PQIAFK

6. Спиридонов М. С. Технологии искусственного интеллекта в уголовно-процессуальном доказывании // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 481-497. EDN ACSQXH

7. Устинкин П. А. Допрос с использованием систем видеоконференцсвязи. URL: https://cyberleninka.ru/article/n/dopros-s-ispolzovaniem-sistem-videokonferentssvyazi/viewer

Е. И. Дискин,
кандидат юридических наук,
Национальный исследовательский университет
«Высшая школа экономики»

РЕГУЛИРОВАНИЕ ИНТЕРНЕТ-ПЛАТФОРМ – НОВЫЕ ВЫЗОВЫ ДЛЯ СТРАН БРИКС

Аннотация. Регулирование интернет-платформ представляет собой сложный вызов. Опыт показывает, что зачастую власть, которой обладают транснациональные корпорации, контролирующие интернет-платформы, может быть большей, чем власть отдельных государств в киберпространстве. Объединение БРИКС после своего расширения получает уникальный шанс использовать свою власть для формирования более справедливого миропорядка, в котором будет учтено мнение государств глобального Юга относительно регулирования интернет-пространства. В условиях, когда государства – члены G7 переходят к комплексному регулированию интернет-платформ, что включает в себя такие аспекты, как модерация, алгоритмы, права пользователей, транспарентность работы социальных сетей, поисковых и аудиовизуальных сервисов, государства БРИКС также должны предпринять аналогичные усилия, чтобы защитить права своих граждан и суверенитет в киберпространстве.

Ключевые слова: право, цифровые технологии, БРИКС, регулирование интернет-платформ, цифровое право, Интернет

REGULATION OF THE INTERNET PLATFORMS – NEW CHALLENGES FOR THE BRICS COUNTRIES

Abstract. Regulating Internet platforms is complex and challenging. Experience shows that often the power of transnational corporations to control Internet platforms may be greater than that of the individual States in cyberspace. After expansion the BRICS gets a unique opportunity to use its power to shape a more equitable world order that takes into account the views of the global South on the regulation of Internet space. As the G7 member states move towards integrated regulation of Internet platforms, which includes such aspects as moderation, algorithms, user rights, transparency of social networks, search and audio-visual services, BRICS States should also make similar efforts to protect the rights of their citizens and sovereignty in cyberspace.

Keywords: Law, Digital Technologies, BRICS, Regulation of Internet Platforms, Digital Law, Internet

Введение. Развитие интеграции стран БРИКС, как и любой подобный процесс, имеет свои сильные и слабые стороны. На текущий момент взаимодействие между государствами – участниками данного объединения не имеет в фокусе ряд новых направлений регулирования киберпространства, таких как вопросы регулирования интернет-платформ. Это приводит к ухудшению положения каждого из участников объединения на международной арене в части возможностей влияния

на глобальные корпорации, такие как Google, Microsoft, Meta* (признана экстремистской организацией, ее деятельность запрещена на территории Российской Федерации) или X (бывший Twitter, социальная сеть, заблокированная на территории РФ за распространений незаконной информации, ее деятельность запрещена на территории Российской Федерации).

Изменения в законодательном подходе к регулированию интернет-платформ происходят буквально на наших глазах. Принятие такого всеобъемлющего нормативного акта, как Регламент Европейского парламента и Совета ЕС 2022/2065 от 19 октября 2022 г., сокращенно именуемого «Закон о цифровых услугах» (Digital Services Act, DSA), знаменует собой смену глобальной парадигмы регулирования. Доктрина «невмешательства» в деятельность интернет-платформ, попытки ограничиться лишь инструментами антимонопольного права, когда такие компании рассматриваются как доминирующие на цифровых рынках, признаны недостаточными, что в свою очередь потребовало разработки, по сути, кодифицированного нормативного акта, определяющего порядок предоставления цифровых услуг в странах ЕС.

На смену упомянутой парадигме «невмешательства» приходит новая эра [1] – эра всеобъемлющего регулирования цифровой среды, эра цифровых кодексов, когда законодательному регулированию будут подвергнуты практически все аспекты деятельности интернет-платформ, закреплены права пользователей киберпространства, введена ответственность за ряд правонарушений, которые еще несколько лет назад не признавались таковыми.

1. Рамки сотрудничества стран БРИКС в области цифровых технологий

В вопросах цифрового регулирования страны БРИКС, очевидно, движутся на разных скоростях. В частности, если рассмотреть концептуальные заметки к саммиту государств БРИКС в 2022 году, то слово «цифровой» (digital) упоминается не так уж часто – всего семь раз [2]. Причем ни одно из упоминаний не относится к взаимодействию за пределами вопросов цифровых инноваций и цифровой экономики. Однако сами по себе интернет-платформы и проблема их регулирования в кооперации государств – членов БРИКС уже не является вопросом развития инноваций как таковых. В частности, авторы доклада для дискуссионного клуба «Валдай» за июнь 2021 года «Мир платформ: от корпораций к регионам» отмечают, что «на корпоративном уровне технология платформенной бизнес-модели явно прошла первые стадии инноваций и сейчас активно переходит к стадии тиражирования в разных отраслях и географических регионах» [3. С. 5]. Таким образом, назревающий вопрос всестороннего регулирования интернет-платформ уже не является вопросом только экономики или развития и стимулирования инноваций, так как растет значимость данных правоотношений с политической и социальной точки зрения.

Согласно докладу 2019 года компании McKinsey, уже в 2025 году интернет-платформы будут формировать до 30 % доходов всех мировых корпораций, что составит примерно 60 трлн долларов [4]. Это означает, что интернет-платформы являются фактором сегодняшнего дня и нуждаются в регулировании всех основных направлений их деятельности, так как их влияние на распространение

информации постоянно и неуклонно растет: число ежемесячных пользователей Facebook* (признана экстремистской, ее деятельность запрещена на территории Российской Федерации) в январе 2023 года достигло почти 3 млрд человек, пользователей YouTube – 2,5 млрд, TikTok ежемесячно просматривает 1 млрд человек [5].

18 марта 2015 года правительствами государств БРИКС был подписан Меморандум о сотрудничестве в сфере науки, технологий и инноваций [6]. Статья 3 данного Меморандума указывает на сферы сотрудничества, в которых, к сожалению, отсутствует соответствующее направление взаимодействия – как исследования в области регулирования интернет-платформ, так и, соответственно, само регулирование. В статье 4 Меморандума описаны модальности работы в рамках сотрудничества, которые включают обмен учеными, исследователями и обучающимися, развитие человеческого капитала в науке, технологиях и инновациях, проведение совместных научных мероприятий, обмен научной и технологической информацией, формулирование общих исследовательских механизмов и формирование их общего финансирования. В том же году была создана Рамочная программа БРИКС в области науки, технологий и инноваций, утвержденная Московской декларацией государств – членов БРИКС от 28 октября 2015 года [7]. Согласно заявлению Уфимской декларации стран БРИКС целью указанной программы является «финансирование совместных многосторонних проектов в сфере научных исследований, коммерциализации технологий и инноваций, с привлечением министерств и центров науки и технологий, институтов развития, а также национальных и при необходимости региональных фондов, осуществляющих финансирование научно-исследовательских проектов» [8].

Исследователи отмечают, что взаимодействие между странами БРИКС в этой сфере пока «скорее риторика, чем реальность» [9. С. 155]. Возможно, это не совсем объективная оценка, однако лучшим опровержением таких заявлений будет усиление кооперации между странами БРИКС. В свою очередь, отметим, что в странах БРИКС появляется осознание необходимости регулирования интернет-платформ как фактора политической и социальной стабильности. В частности, в упомянутом докладе Международного дискуссионного клуба «Валдай» подчеркивается мысль, что «блокировка аккаунта действующего американского президента компаниями Twitter, Facebook* (социальные сети, заблокированные на территории РФ за распространений незаконной информации, их деятельность запрещена на территории Российской Федерации). и другими крупными социальными сетями говорит не только о том, насколько мощными стали определенные платформы, но и о необходимости надлежащего управления этими платформами и их регулирования» [3. С. 9]. Нельзя не согласиться и с мыслью о том, что «платформы основных социальных сетей стали играть настолько жизненно важную роль в современном обществе, что фактически превратились в коммунальные службы и могут рассматриваться как часть важнейшей коммуникационной инфраструктуры той или иной страны» [3. С. 9]. Проблема в том, что на текущий момент данная «коммунальная инфраструктура» в значительной мере не обращает внимания на законные требования государств-членов БРИКС.

В отношении крупнейших иностранных интернет-платформ в России вынесены десятки решений о назначении штрафов на десятки миллиардов рублей. Facebook, Instagram, LinkedIn (социальные сети, заблокированные на территории РФ за распространений незаконной информации, их деятельность запрещена на территории Российской Федерации) подвергнуты блокировке по различным основаниям – первые за экстремистскую деятельность, последняя за нежелание локализовать в России персональные данные пользователей. Тем не менее данные меры практически никак не повлияли на изменение подхода и поведения данных платформ по одной простой причине – они знают, что для населения России они остаются востребованными и многие будут продолжать пользоваться ими с помощью VPN. В этом смысле заявления депутата Государственной Думы, заместителя председателя комитета по информационной политике, информатизации и связи Антона Горелкина о том, что «иностранные сервисы обязательно будут соблюдать новые правила, но позже» [10], выглядят излишне оптимистично. Пока никаких предпосылок для этого не наблюдается, скорее, наоборот – мы видим создание новой реальности, в которой иностранные интернет-платформы переходят в серую зону и перестают соблюдать какие-либо требования российского законодательства. Так, в частности, корпорация Google предпочла провести банкротство своего российского подразделения – ООО «Гугл», нежели выполнять многочисленные требования российских судов по ряду исков и производств по делам об административных правонарушениях [11]. В свою очередь, Facebook и Instagram (социальные сети, заблокированные на территории РФ за распространений незаконной информации, их деятельность запрещена на территории Российской Федерации) не предприняли никаких значимых действий для прекращения политики, послужившей основанием для признания их действий экстремистскими [12].

2. Совместное регулирование интернет-платформ

Учитывая интенсификацию интеграционных процессов и увеличение числа государств – членов БРИКС, расширение совместной повестки в области регулирования интернет-платформ может представлять большой интерес. Рост влияния БРИКС в его новом, расширенном формате открывает возможности для форм сотрудничества, которые направлены на формирование нового, более справедливого мирового порядка, в котором государства глобального Юга будут иметь значительно большее влияние на ключевые процессы в мировой экономике и политике.

На указанное обстоятельство обратили внимание участники Международного форума инноваций БРИКС, который прошел в Москве с 27 по 30 августа 2023 года. В частности, в рамках пленарной сессии «Город для инноваций. Саммит институтов развития» исполнительный директор некоммерческой организации Digital Pilipinas Амор Макланг заявила, что после расширения круга участников БРИКС никто не сможет игнорировать государства, входящие в состав объединения, так как их совокупное население составляет миллиарды человек. С этим тезисом следует согласиться, так как модель монетизации интернет-платформ в основном строится на постоянном увеличении числа пользователей в рамках freemium-модели

монетизации [13], что, в свою очередь, невозможно без вовлечения жителей стран БРИКС. Необходимо также принять во внимание, что синхронно с расширением состава БРИКС и включением в него Аргентины, Ирана, Саудовской Аравии, Египта, ОАЭ и Эфиопии председательство в данной организации переходит к России, что дает возможность представить данную инициативу для совместной работы и привлечь к ней повышенное внимание.

В рамках создания новых механизмов и направлений взаимодействия между государствами БРИКС следует учитывать значительный накопленный опыт некоторых участников объединения в данной области регулирования. Можно выделить особый опыт государств Латинской Америки, таких как Аргентина и Бразилия, которые достаточно давно отмечают необходимость большего вовлечения развивающихся стран в процесс глобального управления сетью Интернет [14. С. 13]. Не менее важным представляется опыт Индии и Китая, концептуально разный, но одинаково важный для будущего глобальной Сети. К совместной работе должны быть привлечены государства Африки – ЮАР и Эфиопия, а также такие новые члены БРИКС, как Иран и Саудовская Аравия.

Заключение. Синхронизация регуляторной повестки между государствами с разными культурными и правовыми традициями представляет собой сложную задачу. Обновленное объединение БРИКС, в которое в 2024 году вступят Аргентина, Египет, Иран, ОАЭ, Саудовская Аравия и Эфиопия, станет гораздо более представительным с точки зрения репрезентации государств глобального Юга. Такое масштабное расширение дает России шанс на то, чтобы на самом раннем этапе работы в расширенном составе задать тон для продуктивной работы в интересах всех участников.

Формирование более справедливого миропорядка невозможно без основанного на мультилатерализме учета мнения большей части населения земного шара по вопросам регулирования интернет-платформ, которые охватывают его своими услугами. Невозможно считать справедливым положение, когда государственный суверенитет не распространяется на интернет-пространство, а для прекращения правонарушений, совершаемых на крупных интернет-платформах, необходимо порой полное отключение Интернета на определенный промежуток времени. Лишь совместная работа членов БРИКС может оказать влияние на платформы, которые будут поставлены перед риском лишиться доступа к миллиардам существующих и новых пользователей.

Список литературы

1. Neves I. From the Digital Services package to the Digital Markets Act: the road to a (more) secure, open, and fundamental rights-friendly digital space. The official blog of UNIO- EU Law Journal. URL: https://officialblogofunio.com/2023/05/04/from-the-digital-services-package-to-the-digital-markets-act-the-road-to-a-more-secure-open-and-fundamental-rights-friendly-digital-space

2. XIV BRICS Summit. Concept Paper on Thematic Issues. URL: http://brics2022.mfa.gov.cn/eng/zg2022/CPTI/

3. Лисоволик Я., Мок Э., Степанова А. Мир платформ: от корпораций к регионам: доклад Международного дискуссионного клуба «Валдай», июнь 2021 г. URL: https://ru.valdaiclub.com/a/reports/mir-platform-ot-korporatsiy-k-regionam/

4. Platforms and Ecosystems: Enabling the Digital Economy. Briefing Paper. World Economic Forum. URL: https://www.weforum.org/whitepapers/platforms-and-ecosystems-enabling-the-digital-economy

5. Most popular social networks worldwide as of January 2023, ranked by number of monthly active users (in millions). Statista. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

6. Меморандум о сотрудничестве в сфере науки, технологий и инноваций между государствами – членами БРИКС от 18 марта 2015 г. URL: http://mniop.ru/wp-content/uploads/2019/11/Memorandum-o-sotrudnichestve-i-vzaimoponimanii-v-sfere-nauki-tehnologii---i-innovatsii--.pdf

7. BRICS STI Framework Programme. URL: http://brics-sti.org/?p=new/32

8. Уфимская декларация (Уфа, Российская Федерация, 9 июля 2015 года). URL: https://clck.ru/re45r

9. Кан М. Перспективы сотрудничества стран БРИКС в области науки, технологий и инноваций // Вестник международных организаций: образование, наука, новая экономика. 2015. Т. 10, № 2. С. 155-185.

10. Как будет работать закон о рекомендательных алгоритмах // Парламентская газета. URL: https://www.pnp.ru/economics/kak-budet-rabotat-zakon-o-rekomendatelnykh-algoritmakh.html

11. Российская «дочка» Google подала заявление о банкротстве. URL: https://www.rbc.ru/business/17/06/2022/62ac165d9a794786f5c8128e

В России признали экстремистскими и запретили Facebook и Instagram // РБК. URL: https://www.rbc.ru/politics/21/03/2022/623882d99a79476d9ca054ab

12. Josimovski S., Pulevska Ivanovska L., Kiselicki M. Implementing the freemium business model in the software industry: key findings and implications. Conference: Contemporary Trends and Multidisciplinary Issues in Social Sciences. URL: https://www.researchgate.net

13. Aguerre C. Internet Governance Networks at National Level. Experience of Recent Cases in Latin America. Towards an Internet Free of Censorship II Perspectives in Latin America. Buenos Aires, 2017.

Е. В. Киенко
кандидат юридических наук,
Дипломатическая академия Министерства иностранных дел
Российской Федерации

НЕКОТОРЫЕ ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПЛАВАНИЯ МОРСКИХ АВТОНОМНЫХ (БЕЗЭКИПАЖНЫХ) СУДОВ

Аннотация. Ключевой международной организацией, занимающейся разработкой международных конвенций и других международных правовых документов, регулирующих плавание автономных (безэкипажных) судов, является Международная морская организация. Заинтересованные в эксплуатации таких судов государства имплементируют новые нормы в свое национальное законодательство, реализуют в соответствии с ними проекты. В будущем для эффективного и безопасного морского автономного (безэкипажного) судоходства предстоит решить целый ряд вопросов: привести юридические термины к единообразию, внести изменения в существующие конвенции, разработать и принять новые международные документы (как обязательного, так и рекомендательного характера), регулирующие специальные вопросы осуществления безэкипажного судоходства, преодолеть технические трудности и т. д.

Ключевые слова: морские автономные (безэкипажные) суда, судоходство, Международная морская организация, искусственный интеллект

SOME ISSUES OF LEGAL REGULATION OF MARITIME AUTONOMOUS SURFACE SHIPS NAVIGATION

Abstract. The International Maritime Organization (IMO) is the key international organization involved in the development of legal instruments regulating the navigation of maritime autonomous surface ships. Some States interested in navigation integrate new norms into their national legislation and fulfil projects. In the future, some issues should be solved to provide effective and safe navigation: legal terms should be harmonized, some applicable IMO conventions should be amended, new (binding or non-binding) international agreements regulating special issues of navigation should be developed and adopted, the technical difficulties should be overcome, etc.

Keywords: maritime autonomous (crewless) surface ships, shipping, the International Maritime Organization, artificial intelligence

Введение. По прогнозам, опубликованным Российским университетом транспорта, выход в море первых коммерческих рейсов на автономных (безэкипажных) судах на дистанционном управлении ожидается к 2025 г., частично управляемых бортовым искусственным интеллектом (далее – ИИ) – к 2030 г. и полностью автономных (безэкипажных) судов, управляемых ИИ, к 2035 г. [7].

Активное развитие автоматизации морского транспорта не только открывает новые возможности для коммерческих морских перевозок, но и влечет за собой

серьезные изменения в жизни общества. Согласно имеющимся данным, автоматизация на судах позволит в значительной мере снизить число несчастных случаев на море, сократить затраты на содержание экипажа, повысить энергоэффективность за счет сокращения расхода топлива, а также предотвратить пиратство [Гаврилов В. В., Дремлюга Р. И. Актуальные вопросы международно-правового регулирования плавания морских судов без экипажа. Московский журнал международного права. 2020. № 2. С. 65-76.

Активное развитие автоматизации морского транспорта не только открывает новые возможности для коммерческих морских перевозок, но и влечет за собой серьезные изменения в жизни общества. Согласно имеющимся данным, автоматизация на судах позволит в значительной мере снизить число несчастных случаев на море, сократить затраты на содержание экипажа, повысить энергоэффективность за счет сокращения расхода топлива, а также предотвратить пиратство [7]. При этом использование автономного морского транспорта не лишено определенных недостатков, в частности, касающихся трудовой занятости квалифицированных кадров, возможных технических сбоев в системе ИИ, кибербезопасности морских судов.

Для урегулирования этих вопросов необходимо, в том числе совершенствовать нормативно-правовую базу.

Основная часть. В нормативных документах разного уровня, а также в правовой литературе встречаются разные понятия, обозначающие морское автономное (безэкипажное) судно: «морское автономное надводное судно», «морское безэкипажное судно», «беспилотные надводные корабли», «суда без экипажа», «беспилотные суда» и т. д.

В документах, разработанных под эгидой Международной морской организации (далее – ИМО), принято обозначать такие суда, как «*maritime autonomous surface ship (MASS)*» или «морское автономное надводное судно (МАНС)», «которое в той или иной степени может функционировать независимо от взаимодействия с человеком» [10].

В отечественной правовой литературе чаще встречаются «беспилотные суда», «безэкипажные суда», «суда без экипажа». Как отмечает профессор В. Н. Гуцуляк, «термин «автономные» является не вполне удачным по отношению к судам без экипажей, потому что под определением «автономность» более привычно подразумевать срок плавания без пополнения запасов» [5]. Для упрощения понимания в статье мы будем придерживаться понятия «морское автономное судно», так как оно уже распространено в международной практике.

В настоящее время пока не сложилось единого мнения и в отношении уровней автономности судов, который зависит от степени вмешательства человека в работу судна. Так, например, в документах ИМО выделяются четыре уровня автономности (с 3-го уровня на борту судна нет экипажа – дистанционно управляемое судно; уровень 4 – полностью автономное судно, т. е. операционная система судна способна сама принимать решения и предпринимать действия) [10]. В российском законодательстве, в зависимости от конкретного нормативно-правового акта, наблюдается иная классификация, которая будет приведена далее.

В рамках ИМО разработкой специальных руководств, стратегических планов, а также международных документов, касающихся МАНС и относящихся к их компетенции, занимается специально созданная Рабочая группа, состоящая из трех комитетов – Комитет по безопасности на море (*Maritime Safety committee*), Юридический комитет (*Legal Committee*) и Комитет по упрощению формальностей (*Facilitation Committee*). Перед Рабочей группой поставлена задача по оценке существующих международных договоров ИМО на предмет их применимости к МАНС и наличия пробелов, препятствующих их эксплуатации. С 2017 г. Комитет по безопасности на море ИМО проводит работу по анализу договоров по безопасности судов с целью определения того, каким образом в документах, принятых под эгидой организации, могут быть отражены вопросы безопасного, надежного и экологичного функционирования МАНС. В результате предложено разработать новый документ по МАНС, а именно – Кодекс, содержащий правила, которые подойдут для всех четырех степеней автономности.

В апреле 2022 г. в Комитете по безопасности на море на 105-й сессии одобрен план работ, предполагающий последовательную разработку общих принципов, приоритетных направлений работ, терминологии, а также разработку международного Кодекса по МАНС рекомендательного характера к 2026 г. Заявлено, что действие документа будет распространяться также на грузовые и рыболовные суда. В июне 2023 г. на 107-й сессии Комитета по безопасности на море было решено, что к 2028 г. Кодекс будет принят в качестве обязывающего договора, который восполнит правовые пробелы в Международной конвенции по охране человеческой жизни на море 1974 г. [11].

Помимо разработки нового международного документа, целесообразно адаптировать уже принятые универсальные международные «морские» конвенции: Конвенцию ООН по морскому праву 1982 г., Международную конвенцию по охране человеческой жизни на море 1974 г., Международную конвенцию по предотвращению загрязнения с судов 1973–1978 гг., Международную конвенцию о подготовке и дипломировании моряков и несении вахты 1978 г., Международную конвенцию по поиску и спасанию на море 1979 г., Международную конвенцию по безопасным контейнерам 1972 г., Международную конвенцию по облегчению международного морского судоходства 1965 г., Международные правила предупреждения столкновения судов в море 1972 г. и др.

Более конкретно, существенные изменения могут затронуть те нормы, которые регулируют вопросы деятельности экипажа на борту, спасания, ответственности, морского страхования и т. д. Так, например, в Конвенции ООН по морскому праву 1982 г. под пересмотр попадают ст. 27 («Уголовная юрисдикция на борту иностранного судна»), ст. 97 («Уголовная юрисдикция в случае столкновения или какого-либо другого навигационного инцидента»), ст. 98 («Обязанность оказания помощи»), ст. 211 («Загрязнение с судов»), ст. 292 («Незамедлительное освобождение судна и экипажа») и другие. В Международной конвенции по охране человеческой жизни на море 1974 г. изменения коснутся целого ряда дефиниций, технической документации, выдачи свидетельств и перечней оборудования и т. д. В Международной конвенции по предотвращению загрязнения с судов (МАРПОЛ)

1973 – 1978 к таким нормам относится ст. 6 («Обнаружение нарушений и осуществление Конвенции»). Наиболее значительные изменения потребуются в отношении переквалификации моряков и появлении новых специальностей (в частности, берегового капитана), т. е. Международной конвенции о подготовке и дипломировании моряков и несении вахты 1978 г.

Возможно, что в будущем при заметном росте численности автономного флота потребуется также разработать новый международный документ, который поможет разрешить технические проблемы по обеспечению согласованности при взаимодействии беспилотных объектов между собой и в группе [7]. При этом необходимо учитывать их типы, размеры, каналы связи и т. д.

Система управления автономными судами неразрывно связана с ИИ, что порождает новые сложности, связанные с правовым регулированием их деятельности. По мнению отечественных юристов-международников, этот вопрос невозможно решить простым переносом норм на новые субъекты – системы ИИ или на сами автономные суда [1. С. 71]. Соответственно, в будущем исследователи прогнозируют выделение ИИ в качестве самостоятельного субъекта права [1. С. 71]. Помимо этого, с появлением автономных судов возникает и реальная угроза их кибервзлома злоумышленниками. Несмотря на существование конвенций, регулирующих вопросы противодействия киберпреступности, предлагается принять новый Международный договор по кибербезопасности МАНС [1. С. 73].

Вместе с тем сегодня многие из этих вопросов уже решены на международном уровне. Результатом 107-й сессии Комиссии по безопасности на море ИМО стало принятие новых изменений к Главам II-1, II-2, XIV Международной конвенции по охране человеческой жизни на море и Протоколам к ней; Кодексам безопасности высокоскоростных судов 1994 г. и 2000 г., Полярному кодексу, а также к Международной конвенции о подготовке и дипломировании моряков и несении вахты [11].

По имеющимся данным, по состоянию на 2021 г. ни одно государство не имеет коммерческого автономного флота [7]. Тем не менее солидное число государств развивает свое внутреннее законодательство на перспективу внедрения МАНС.

Российская Федерация активно формирует нормативную базу в области автономного судоходства. В российское законодательство, касающееся вопросов морского транспорта и эксплуатации судов, уже внесены значительные изменения. Федеральным законом от 10.07.2023 № 294-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (о правовом регулировании эксплуатации автономных судов) вводится понятие «автономное судно». Под автономным судном понимается самоходное судно, процессы управления которым в зависимости от наличия или отсутствия экипажа на борту судна частично (полуавтономное судно) или полностью (полностью автономное судно) осуществляются в автоматическом режиме. Под полуавтономным судном понимается судно с экипажем на борту, способное осуществлять плавание без непрерывного несения ходовой вахты экипажем. Под полностью автономным судном понимается судно, способное осуществлять плавание без экипажа на борту [9]. При этом плавание автономных иностранных военных кораблей и других автономных государственных судов, эксплуатируемых в некоммерческих целях, во внутренних морских водах и в территориальном море

запрещается, за исключением случаев плавания таких автономных иностранных военных кораблей и других автономных государственных судов с разрешения федерального органа исполнительной власти в области обороны в сопровождении и в соответствии с указаниями командира военного корабля Российской Федерации [9]. Таким образом, в Кодекс торгового мореплавания Российской Федерации, федеральные законы «О внутренних морских водах, территориальном море и прилежащей зоне Российской Федерации», «О транспортной безопасности» и другие документы были внесены изменения, касающиеся эксплуатации автономных судов.

В 2021 г. принята Транспортная стратегия РФ на период до 2030 года с прогнозом на период до 2035 года (утверждена распоряжением Правительства Российской Федерации от 27 ноября 2021 г. № 3363-р), которая предполагает внедрение технологий автономного транспорта не только в морском, но и во внутреннем водном судоходстве. В рамках развития автономного водного транспорта запланировано внедрение автономных судов в пассажирских и грузовых перевозках (с уровнем автономности 2 и выше). Для этих целей прогнозируется связанное с судоходством ускоренное развитие инфраструктуры интернета вещей и навигационных технологий [8]. В Приложении 10 к Транспортной стратегии указаны 7 степеней автономности судов (от 0 – когда автоматизация отсутствует, все процессы выполняются с привлечением человека; до 6 – все решения полностью принимаются и реализуются системой) [8].

Президентом Российской Федерации В. В. Путиным поставлены задачи обеспечить регулирование правоотношений, возникающих при использовании безэкипажного (автономного) судовождения, а также провести в период 2021–2025 гг. эксперимент по опытной эксплуатации безэкипажных (автономных) судов, плавающих под Государственным флагом РФ [6].

Заключение. Правовое регулирование автономных (безэкипажных) судов находится на начальном этапе формирования. Государствам еще предстоит договориться о понятийном аппарате, адаптировать действующие международные договоры и свое внутреннее законодательство к технологическим изменениям, происходящим в транспортной сфере, выработать общие подходы к решению технических проблем, а также установить квалификационные требования к «береговым» специалистам, которые будут заниматься управлением автономных судов с берега. Развитие нормативно-правовой базы МАНС происходит заблаговременно. Пока же моряки по-прежнему незаменимы для безопасного судоходства.

Список литературы

1. Гаврилов В. В., Дремлюга Р. И. Актуальные вопросы международно-правового регулирования плавания морских судов без экипажа. Московский журнал международного права. 2020. № 2. С. 65-76.

2. Конвенция ООН по морскому праву 1982 г. // ООН. URL: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_r.pdf

3. Международная конвенция по охране человеческой жизни на море (СОЛАС) 1974 г. // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/901765675

4. Международная конвенция по предотвращению загрязнения с судов (МАРПОЛ) 1973/78 г. // Электронный фонд правовых и нормативно-технических документов. URL: https://docs.cntd.ru/document/901764502

5. Морские суда без экипажей – реальность и перспективы: сборник научных докладов по итогам «круглого стола», проводимого совместно кафедрой «Морское право» Юридического института Российского университета транспорта (РУТ) и Ассоциацией международного морского права / под редакцией В. Н. Гуцуляка. Москва: Юридический институт РУТ (МИИТ), 2020. 41 с.

6. Постановление Правительства РФ от 5 декабря 2020 г. «О проведении эксперимента по опытной эксплуатации автономных судов под Государственным флагом РФ» // Гарант.ру. URL: https://www.garant.ru/products/ipo/prime/doc/74916791/

7. Состояние дел и перспективы автономного судоходства. Дайджест. Якунчиков В.В., Алферов В.В., Ходько С.Н. // Российский университет транспорта, 2021. URL: https://www.miit.ru/content/900756.pdf?id_wm=900756

8. Транспортная стратегия РФ на период до 2030 г. с прогнозом на период до 2035 г. – URL: https://rosavtodor.gov.ru/docs/transportnaya-strategiya-rf-na-period-do-2030-goda-s-prognozom-na-period-do-2035-goda

9. Федеральный закон от 10.07.2023 № 294-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» (о правовом регулировании эксплуатации автономных судов). URL: http://publication.pravo.gov.ru/Document/View/0001202307100007?index=3

10. International Maritime Organization. Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (Mass) MSC.1/Circ.1638 3 June 2021. URL: https://wwwcdn.imo.org/localresources/en/MediaCentre/HotTopics/Documents/MSC.1-Circ.1638%20-%20Outcome%20Of%20The%20Regulatory%20Scoping%20ExerciseFor%20The%20Use%20Of%20Maritime%20Autonomous%20Surface%20Ships...%20(Secretariat).pdf

11. International Maritime Organization. Maritime Safety Committee (MSC 107), 31 May-9 June 2023. URL: https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-107th-session.aspx

Д. В. Лобач,
кандидат юридических наук, доцент,
Дальневосточный юридический институт (филиал)
Университета прокуратуры Российской Федерации

ДЕСТРУКТИВНОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ КАК ФАКТОР ОСЛОЖНЕНИЯ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ

Аннотация. В статье изучается деструктивное использование информационно-коммуникационных технологий в фокусе международных отношений. Отмечается, что в современных условиях цифровой трансформации социальных отношений применяются две модели использования информационно-комму-

никационных технологий в целях осложнения международных отношений: информационная пропаганда и кибернетические атаки. Обосновывается позиция, в соответствии с которой допускается возможность рассмотрения информационно-коммуникационных технологий как применение силы, что предполагает концептуально-правовое расширение понятия силы в международных отношениях. Анализ стратегических документов РФ, США и КНР позволяет заключить, что деструктивное использование информационно-коммуникационных технологий в международных отношениях рассматривается как объективный фактор их осложнения.

Ключевые слова: информационно-коммуникационные технологии, ИКТ, информационное пространство, кибератаки, международные отношения

DESTRUCTIONAL USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES AS A FACTOR OF COMPLICATION OF INTERNATIONAL RELATIONS

Abstract. The article examines the destructive use of information and communication technologies (ICT) in the focus of international relations. It is noted that in modern conditions of digital transformation of social relations, two models of using ICT are used to complicate international relations: information propaganda and cyber attacks. The position is substantiated, according to which the possibility of considering ICT as the use of force is allowed, which implies a conceptual and legal expansion of the concept of force in international relations. An analysis of the strategic documents of the Russian Federation, the United States and China allows us to conclude that the destructive use of ICT in international relations is considered as an objective factor in their aggravation.

Keywords: information and communication technologies, ICT, information space, cyberattacks, international relations

Научно-технический прогресс и процессы глобализации в современном мире предопределяют трансформацию социальных отношений, выражаемую в придании им особой цифровой формы реализации и их интеграции в информационное пространство. Социальные отношения приобретают новые формы выражения, опосредуемые активным и широким распространением информационно-коммуникационных технологий (далее – ИКТ). Действительно, сегодня мы видим, что медицина, транспорт, финансы, образование, социальные услуги, государственное управление, документооборот, досуг (отдых и развлечения) переходят в электронные системы, упрощающие социальное взаимодействие, минимизирующие риски и трансакционные издержки, обеспечивающие относительную безопасность.

Не являются исключением и политические процессы, протекающие как в сфере внутригосударственных политических отношений, так и на международном уровне. Особое внимание обращает на себя качественное преобразование практики международных отношений в условиях развития ИКТ, что проявляется не только в положительных тенденциях и закономерностях, но и в деструк-

тивных процессах, которые детерминируют осложнение международных отношений. Анализ современных тенденций, актуализированных в информационном пространстве в фокусе кризиса международного правового порядка, девальвации международного права и обострения геополитических интересов, позволяет выделить два ключевых направления деструктивного использования ИКТ, создающих угрозу для стабильности международных отношений и всего мирового порядка.

Прежде всего хотелось бы отметить использование современных ИКТ в целях манипулирования общественным сознанием и создания негативного образа того или иного государства. На примере беспрецедентного санкционного давления и открытой информационной агрессии в отношении отдельных государств (Российская Федерация, Иран, КНДР, Венесуэла), проводимой США и их европейскими сателлитами, можно видеть, как в информационном пространстве намеренно и последовательно искажается работа государственных органов, их представителей, а также деятельность общественных институтов. Распространяемая в информационно-коммуникационном пространстве информация посредством использования контекстных вставок, умолчания, открытой фальсификации отдельных фактов, искажения истории демонстрирует ориентацию на создание негативного образа целых государств в современных условиях, что закономерным образом подрывает авторитет государства на международной арене и приводит к снижению патриотических настроений в самом обществе. Обращает на себя внимание не только содержание такой информации, но и форма и способы ее подачи и ретрансляции. Как правило, это небольшие по времени видеоролики, в которых используются непроверенные статистические данные, демонстрирующие, как правило, отрицательную динамику и негативные тенденции; оценки событий со стороны лиц, позиционирующих себя в качестве экспертов; искаженные исторические факты; мультипликационные заставки; театральные постановки; компьютерная графика; недопустимые сравнения (ложная аналогия) [4]. Часто такая информация подается под видом проведенных научных исследований и искусственно создается референтная аудитория.

Наиболее распространенными акцентами в дезинформации, используемой для того, чтобы дискредитировать, занизить исторический вклад в развитие мировой цивилизации и подорвать социокультурное значение какого-либо государственного образования, являются такие маркеры (основная идея или основные контекстные смыслы), как массовые убийства, убийства детей и женщин, агрессия (агрессивная война), геноцид, преступления против человечности, оружие массового поражения, концентрационные лагеря. В свою очередь, акцентирование на негативных смысловых позициях в определяемом дискурсе дезинформации позволяет создавать корректный негативный образ публично-правовых образований, включая государства. Например, сегодня в информационном пространстве против России применяются разные негативные политические образы, которые характеризуют ее как империю зла, государство-агрессор, преступное государство, угрозу человечеству или цивилизации. Это приводит к нагнетанию и обострению отношений в обществе, возникновению недоверия к власти, искажению системы традиционных ценностей и снижению патриотических настроений.

Высокий уровень качества фальсификации вбрасываемого в информационное пространство материала достигается через активное использование технологии deep fake. Под этой технологией понимается система машинного синтезирования аудиовизуального цифрового контента (изображений, аудио, видео и даже текста) с целью создания видоизмененного и при этом максимально реалистичного контента [2]. В специальной литературе справедливо отмечается, что указанная технология обладает повышенной общественной опасностью, поскольку позволяет осуществить распространение экстремистского материала, спровоцировать межэтнические или межконфессиональные конфликты в обществе. Низкий уровень информационной грамотности и отсутствие критического мышления у большинства населения затрудняют возможность верификации распространяемой информации. Отсутствие у населения необходимых знаний и навыков, позволяющих адекватно и безопасно оценивать такую информацию с учетом ее массового распространения такой информации, создает высокие риски осложнения социальных отношений и ставит под угрозу стабильность правового порядка [9]. Ситуация во многом усугубляется еще и тем, что действия государства по разоблачению «глубокой» подделки могут быть запоздалыми в контексте интенсификации социальной напряженности, когда негативная динамика нагнетания переходит в открытую вражду или даже в противостояние.

Другой тенденцией деструктивного использования ИКТ в информационном пространстве является применение искусственного интеллекта (далее – ИИ) для генерации опасного контента. Технологии ИИ позволяют проводить анализ политических ожиданий, моделировать политические предпочтения, выявлять риски в политическом процессе, формулировать разные лозунги и агитационные материалы, осуществлять рассылку таргетированных сообщений, оперативно реагировать на обращения избирателей через использование чат-ботов, а также прогнозировать дальнейшее развитие политических процессов [11]. Не без интереса отметим, что ИИ-сервисы представляют инструменты, позволяющие простому человеку, который не является квалифицированным специалистом в сфере программирования и IT-технологий, создавать и распространять политическую дезинформацию, для того чтобы повлиять на избирателей и (или) саботировать политический процесс [6].

Общественная опасность использования ИКТ в деструктивных целях (манипулирование общественным сознанием для создания негативного образа своего или другого государства) обусловлена тем, что такая практика создает у человека презумпцию достоверности и правильности распространения информационного контента, снижая тем самым критическое мышление и адекватное восприятие. Возникает параллельная действительность, в которую погружается человек, а как следствие – меняется его модель и вектор поведения в соответствии с новыми представлениями о должном и необходимом. Не будет преувеличением сказать, что подобного рода практика использования ИКТ создает политические симулякры, отдаляющие человека от правильного (адекватного) понимания политического процесса в межгосударственном общении.

В свою очередь, расшатывание социального порядка и снижение доверия к власти предопределяет два сценария развития ситуации, связанной с осложне-

нием международных отношений. В рамках первого варианта в результате мобилизации протестных групп возникает осложнение социальных отношений внутри государства, что приводит к несанкционированным шествиям, митингам и другим акциям, нарушающим общественный порядок, которые могут повлечь не только дезорганизацию работы органов и организаций, но и привести к государственному перевороту и изменению самой конфигурации власти. Второй вариант связан с искусственным созданием обстановки массового, систематического и грубого нарушения прав и свобод в обществе в результате проводимой государством дискриминационной политики или открытого террора против отдельных социальных групп. Такой вариант ориентирован на то, чтобы создать условия для применения силы против суверенитета, политической независимости и территориальной целостности другого государства под предлогом защиты населения, проживающего в этом государстве, или предотвращения гуманитарной катастрофы.

ИКТ активно используются не только в пропагандистских целях, но и для непосредственного воздействия на объекты критической инфраструктуры, с тем чтобы подорвать государственный суверенитет или политическую независимость. В современных условиях ни для кого не секрет, что кибернетическое оружие способно причинить реальный физический вред объектам военной и гражданской инфраструктуры. Хорошо известен случай кибератаки против ядерного объекта Ирана, когда запущенный вирус Stuxnet вывел из строя центрифуги для обогащения урана в Иране, замедлив иранскую ядерную программу на несколько лет.

В условиях осложнения международных отношений, усложнения технологического прогресса и интеграции в информационное пространство все большего числа субъектов социального взаимодействия наблюдается усиление напряженности в киберпространстве, что проявляется в кратном увеличении количества кибератак на объекты критической инфраструктуры, органы государственной власти и частный сектор [15]. Эксперты отмечают, что наибольшее количество кибератак на веб-ресурсы 2022 г. пришлось на СМИ, транспорт, государственные учреждения, торговлю и сферу услуг [1]. В условиях осложнения отношений между мировыми державами и конфликта на Украине кибер атаки становятся неотъемлемой частью гибридной войны.

В научной литературе, посвященной изучению современных вызовов и угроз, предпринимаются попытки определения деструктивного использования ИКТ против интересов другого государства как преступление агрессии. Так, некоторые авторы отмечают, что кибер атаки могут подорвать информационную безопасность, парализовать военную инфраструктуру и ослабить экономическую систему не в меньшей степени, чем непосредственное применение вооруженных сил [12]. Если по характеру последствий информационные кибер атаки могут порождать последствия, соотносимые с применением биологического или любого другого вида оружия, то вне зависимости от их правового режима они в юридическом смысле могут подпадать под понятие вооруженной силы [8, 10]. Кроме того, основываясь на позициях, а также на выводах, полученных в результате изучения тематического материала в средствах массовой информации относительно применения информационных и компьютерных технологий в боевых действиях (ме-

тодом контент-анализа в общей сложности было проанализировано 56 научных статей, посвященных данному вопросу), представляется возможным согласиться с предложениями ученых о необходимости расширенного толкования понятия «применение вооруженных сил» в контексте практики международных отношений. Но для квалификации кибер атак в качестве акта агрессии необходимо не только посягательство на объекты критической инфраструктуры другого государства, но и на суверенитет, политическую независимость и территориальную целостность государства при условии возникновения угрозы миру или же наступления длительного и (или) интенсивного вооруженного противостояния.

Между тем не следует интерпретировать понятие «применение вооруженных сил», которое является ядром преступления агрессии, через формы невоенного вмешательства (например, подкуп высших должностных лиц государства, разведывательная деятельность, финансирование оппозиции другими государствами, поставки оружия мятежникам, применение технологий «цветных революций» при кураторстве зарубежных спецслужб и т. д.). Обзор специальной литературы [5, 7] относительно политико-правовой природы невоенного вмешательства позволяет предположить, что использование мягкой силы со стороны других государств может привести к планируемым последствиям с минимизацией рисков при более выгодных условиях. При этом под минимизацией рисков понимается снижение вероятности осуждения мировым сообществом самого вмешательства в дела другого государства, а выгодные условия предполагают снижение материальных, организационных, финансовых и иных затрат, необходимых при проведении полноценной военной операции.

Применение ИКТ в агрессивных целях против суверенитета, политической системы, экономической и социальной инфраструктуры рассматривается на национальном уровне отдельных государств как средство внешней политики, приводящее не только к осложнению международных отношений, но и создающее угрозу для международного правового порядка.

В этом аспекте особый интерес представляют стратегические документы, направленные на обеспечение национальной безопасности. Так, например, в Доктрине информационной безопасности Российской Федерации от 5 декабря 2016 г. понятие информационной безопасности раскрывается не только через внутренние угрозы, но и через внешние (то есть в практике международных отношений). Более подробно связь информационных технологий с негативными тенденциями в международных отношениях отражена в новой Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента РФ от 2 июля 2021 г. № 400 [3]. В документе говорится, что в современных условиях обострения геополитического противостояния ИКТ используются для вмешательства во внутренние дела других государств, а также в целях нарушения территориальной целостности и подрыва суверенитета, что ставит под угрозу международный мир и безопасность. Особую роль в этом плане играет информационно-телекоммуникационная сеть Интернет, в которой активно навязывается искаженный взгляд на исторические факты и современные события, а также в целях дестабилизации общественно-политической ситуации в России распространяется различного рода деструктивный контент (недостоверная информация, заведомо ложная информация, материалы террористических

и экстремистских организаций, призывы к насилию, аморальные идеи). Отмечается, что большинство компьютерных атак на российские информационные ресурсы совершаются с территории других государств, а инициативы России по обеспечению информационной безопасности встречают противодействие со стороны иностранных государств, стремящихся доминировать в глобальном информационном пространстве. О стремлении контролировать информационные ресурсы и установить монопольное положение в сети Интернет также говорится в отношении транснациональных корпораций, которые вопреки нормам международного права вводят цензуру и блокируют альтернативные интернет-платформы.

Неменьший интерес вызывает Стратегия национальной кибербезопасности Соединенных Штатов Америки (США), которая была принята в 2018 г. [13]. В представленной Стратегии в четырех принципах раскрываются основные угрозы, вызовы, тренды, фундаментальные проблемы, а также пути их решения в сфере обеспечения национального киберпространства. В документе неоднократно обращается внимание на связь ИКТ с международными отношениями и международным правопорядком. Среди ключевых угроз в сфере кибербезопасности, обозначенных в Стратегии, можно отметить: подрыв принципа свободного Интернета в международном общении; рост числа хакерских атак как со стороны преступных организаций, так и со стороны отдельных стран (Россим, Ирана и Северной Кореи) в отношении транснациональных компаний, союзников и партнеров США; рост числа инцидентов в киберпространстве, связанных с осуществлением экономического шпионажа и кражами объектов интеллектуальной собственности, которые совершаются по инициативе КНР; увеличение количества негосударственных структур, которые используют киберпространство в преступных целях против США и их союзников, при этом их деятельность прикрывается враждебными государствами.

О связи информационных технологий с развитием международных отношений в сфере обеспечения информационной безопасности также прямо говорится в Национальной стратегии безопасности киберпространства Китайской Народной Республики (КНР), принятой в 2016 г. [14]. В документе закреплено, что развитие международных отношений в сфере обеспечения информационной безопасности и мирного использования киберпространства отвечает общим интересам человечества и международного мира, поэтому все страны должны соблюдать принципы Устава ООН, касающиеся неприменения или угрозы применения вооруженной силы, а также стремиться предотвращать использование информационных технологий в целях, противоречащих поддержанию международной безопасности и стабильности, совместного противодействия гонке вооружений в киберпространстве и предотвращения конфликтов в киберпространстве.

В заключение следует отметить, что международные отношения и политический процесс, как и другие социальные сферы, подвержены информационно-цифровому воздействию. Использование ИКТ в деструктивных целях в информационном пространстве создает опасность, а в отдельных случаях и реальную угрозу для международных отношений и международного правопорядка, так как способствует созданию искаженного представления о политическом процессе и межгосударственном общении.

Список литературы

1. Актуальные киберугрозы: итоги 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022

2. Дипфейк: невинная технология для развлечения или угроза современному обществу? URL: https://russiancouncil.ru/analytics-and-comments/analytics/dipfeyk-nevinnaya-tekhnologiya-dlya-razvlecheniya-ili-ugroza-sovremennomu-obshchestvu

3. О Стратегии национальной безопасности Российской Федерации (утв. Президентом РФ 02.07.2021 № 400). URL: http://publication.pravo.gov.ru/Document/View/0001202107030001

4. Пропаганда в Интернете: какие методы и технологии используются для влияния на общественное мнение. URL: https://www.securitylab.ru/analytics/538491.php

5. Преступность – планетарная проблема: к итогам XI Конгресса ООН по предупреждению преступности и уголовному правосудию / Ю. В. Голик, А. И. Коробеев. Санкт-Петербург: Изд-во Р. Асланова «Юридический центр Пресс», 2006.

6. Тамарович А., Алмаматов А. Искусственный интеллект идет в политику. URL: https://russiancouncil.ru/analytics-and-comments/columns/cybercolumn/iskusstvennyy-intellekt-idet-v-politiku/

7. Ashrafi, M. Evaluation of the velvet revolutions in terms of being a revolution or not (Analysis of the velvet revolutions in comparison to the classical revolutions) // Journal of American Science. 2012. Vol. 8(11). Pp. 250-252.

8. Brownlie, L. International Law and the Use of Force by States. UK: Clarendon. 1963.

9. Byman D. L., Gao Ch., Meserole Ch., Subrahmanian V.S. Deep fakes and international conflict. URL: https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf

10. Dinstein, Y. War, Aggression and Self-Defence. 3rd ed. United Kingdom: Cambridge University Press. 2001.

11. Kumar S. The Future of Deep Fakes in the World of Democratized Artificial Intelligence. URL: https://diplomacybeyond.com/the-future-of-deep-fakes-in-the-world-of-democratized-artificial-intelligence/

12. Lilienthal G., Nehaluddin A. Cyber-attack as Inevitable Kinetic War // Computer Law & Security Review. 2015. Vol. 31, Iss. 3. Pp. 390-400.

13. National Cyber Security Strategy of United States of America. URL: https://digital.library.unt.edu/ark:/67531/metadc1259394/m1

14. National Cyberspace Security Strategy of Chine. URL: https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy

15. The Latest 2023 Cyber Crime Statistics (updated August 2023). URL: https://aag-it.com/the-latest-cyber-crime-statistics

Е. Н. Мельникова,
магистр права, юрисконсульт,
Университет ИТМО

ПРАВОВОЙ РЕЖИМ ПОСТАВЩИКА, ПОСТАВЩИКА БАЗОВОЙ МОДЕЛИ И ПОЛЬЗОВАТЕЛЯ ПРИЛОЖЕНИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ЕС СОГЛАСНО AI ACT

Аннотация. Общественные отношения, складывающиеся по поводу создания и использования приложений искусственного интеллекта нуждаются в правовом регулировании в первую очередь потому, что приложения искусственного интеллекта могут нанести вред (ущерб) жизни, здоровью, имуществу людей и окружающей среде. Справедливое распределение ответственности за такой вред (ущерб) может быть возможно только в случае комплексного правового регулирования прав и обязанностей основных участников жизненного цикла приложений искусственного интеллекта (хотя правовой режим иных участников тоже имеет определенное значение). Первый опыт такого правового регулирования впервые предпринят в ЕС: в 2022–2023 гг. в Европарламент внесены три проекта: регламента (сокращенно именуемый AI Act), директивы об ответственности за искусственного интеллекта, директивы об ответственности за дефектную продукцию. В настоящей работе проанализирован правовой режим поставщика, поставщика базовой модели и пользователя приложений искусственного интеллекта согласно AI Act, который будет установлен в ЕС в случае завершения законодательного процесса принятием регламента.

Ключевые слова: AI Act, обязанности, поставщик, базовая модель, пользователь, разработчик, искусственный интеллект

LEGAL REGIME OF THE SUPPLIER, SUPPLIER THE BASIC MODEL AND USER OF ARTIFICIAL INTELLIGENCE APPLICATIONS IN THE EU ACCORDING TO AI ACT

Abstract. The public relations that are developing regarding the creation and use of Artificial Intelligence applications (hereinafter referred to as «AI») need legal regulation, primarily because AI applications can harm (damage) people's lives, health, property and the environment. A fair distribution of responsibility for such harm (damage) can be possible only in the case of a comprehensive legal regulation of the rights and obligations of the main participants in the life cycle of AI applications (although the legal regime of other participants also has some significance). The first experience of such legal regulation was first undertaken in the EU: in 2022-2023, three drafts were submitted to the European Parliament: regulations (abbreviated as the AI Act), directives on liability for AI, directives on liability for defective products. This paper analyzes the legal regime of the supplier, the supplier of the basic model and the user of AI applications according to the AI Act, which will be established in the EU if the legislative process is completed by the adoption of the regulation.

Keywords: AI Act, responsibilities, provider, foundation model, deployer, developer, user, Artificial Intelligence

Введение. Первые значимые попытки комплексного правового регулирования ИИ предприняты пока только в ЕС: комитеты Европейского парламента по внутреннему рынку и гражданским свободам 11 мая 2023 года согласовали основные положения проекта Предложения о регламенте Европейского Парламента и Совета, устанавливающем гармонизированные правила в области искусственного интеллекта (Закон об искусственном интеллекте) и вносящем поправки в некоторые законодательные акты ЕС (далее – AI Act, регламент) [3]. Поправки, принятые Европейским парламентом по предложению о регламенте, появились 14 июня 2023 года, а уже 20 июня 2023 года на сайте Европейского парламента появился [4] документ на 681 страницах, представляющий собой сравнительный анализ изменений текста AI Act в ходе законодательного процесса; в документе содержатся положения первоначального проекта регламента (Commission Proposal), поправки Европейского парламента от 14 июня 2023 года (EP Mandate) и поправки от 20 июня 2023 года Совета Европейского союза (Council Mandate), при этом Commission Proposal претерпел такие существенные изменения, что от первоначальной редакции проекта регламента мало что осталось. По состоянию на август 2023 года AI Act все еще находится в процессе принятия. Размер настоящей статьи не позволяет здесь привести анализ изменений некоторых ключевых положений регламента в динамике, хотя это представляет определенный интерес. В настоящем докладе в целях сокращения в случае расхождений между положениями EP Mandate и Council Mandate, рассматриваются только положения проекта AI Act в редакции Совета Европейского союза (Council Mandate). Если согласие между Европейским парламентом и Советом Европейского союза будет достигнуто, AI Act установит правовой режим участников жизненного цикла приложений ИИ и тем самым внесет существенный вклад в регулирование гражданско-правовых отношений, возникающих в сфере создания и использования ИИ.

С целью гражданско-правового регулирования ответственности за вред (ущерб), причиненный ИИ, в сентябре 2022 года Европейская комиссия предложила две директивы – Директиву об ответственности за ИИ [5] и Директиву об ответственности за дефектную продукцию [6], которая обновит правила ответственности за продукцию, датируемые 1985 годом («Пересмотренная PLD»). Между двумя указанными директивами и AI Act нет дублирования, документы дополняют друг друга: пересмотренный PLD устанавливает обновленные правила, касающиеся строгой ответственности производителя за дефектную продукцию (ответственность без необходимости доказывать вину), а Директива об ответственности AI рассматривает требования об ответственности, основанные на вине, с целью компенсации ущерба лицам, пострадавшим в результате использования систем ИИ с высоким уровнем риска.

Ожидается, что вместе эти три документа: AI Act и вышеуказанные директивы – установят всеобъемлющий режим правового регулирования ИИ на территории ЕС и частично за ее пределами.

Приложения ИИ в терминологии регламента и директив называются системами искусственного интеллекта, поэтому в дальнейшем в данной работе оба термина будут использоваться как синонимы.

1. Сфера применения AI Act

Сфера действия регламента обозначена в ст. 2. AI Act. Согласно п. 1 ст. 2 AI Act применяется к поставщикам, уполномоченным представителям поставщиков, пользователям, производителям, импортерам и дистрибьюторам, затронутым лицам (affected persons), которые находятся в ЕС и на здоровье, безопасность или основные права которых отрицательно влияет использование системы ИИ, которая размещена на рынки или введена в эксплуатацию в рамках ЕС.

Экстерриториальное действие AI Act проявляется в его применении к разработчикам, поставщикам услуг и предприятиям, учрежденным или расположенным за пределами ЕС, при использовании результатов, производимых приложениями ИИ в ЕС, или когда такие системы собирают или обрабатывают персональные данные физических лиц, находящихся в ЕС или Европейской экономической зоне.

AI Act не применяется (ст. 2 п. 3-5):

– к пользователям – физическим лицам, использующим системы ИИ в личной непрофессиональной деятельности (п. 5c, Council Mandate);

– к компонентам ИИ, предоставляемым по бесплатным лицензиям с открытым исходным кодом, за исключением случаев, когда они размещены на рынке или введены в эксплуатацию поставщиком как часть системы ИИ с высоким уровнем риска или запрещены (раздел II AI Act). Это исключение не применяется к базовым моделям, определенным в ст. 3 (п. 5e, EP Mandate);

– к системам ИИ, которые используются в деятельности, касающейся вооруженных сил, обороны или национальной безопасности (п. 3, Council Mandate);

– к системам ИИ, включая их выходные данные, специально разработанным и введенным в эксплуатацию исключительно с целью научных исследований и разработок (п. 5a, Council Mandate);

– к научно-исследовательской деятельности, касающейся ИИ-систем (п. 5b, Council Mandate);

– к исследованиям и испытаниям систем ИИ до их вывода на рынок или ввода в эксплуатацию, при условии, что эти действия осуществляются с соблюдением основных прав и применимого законодательства ЕС. Это исключение не распространяется на испытания в реальных условиях (п. 5d, EP Mandate).

AI Act не осуществляет непосредственное регулирование правоотношений между участниками жизненного цикла приложений ИИ и потребителями, поскольку системы ИИ в ЕС подпадают под действие законодательства о защите прав потребителей (п. 32a преамбулы, EP Mandate).

Очевидно, что из-под действия регламента выводятся основные значимые сферы применения ИИ, развитие которых влияет на цифровой суверенитет государства.

2. Классификация приложений ИИ по уровням риска в AI Act

В AI Act приложения ИИ классифицируются по уровням риска, в зависимости от сферы действия и степени потенциальной опасности, которую система ИИ может представлять для человека и окружающей среды.

Уровень 1. Неприемлемый риск

Системы ИИ с неприемлемым риском запрещены. Они включают в себя те, которые допускают:

– когнитивно-поведенческое манипулирование людьми или конкретными уязвимыми группами;

– социальную оценку, классификацию людей на основе поведения, социально-экономического статуса или личных характеристик;

– системы биометрической идентификации в режиме реального времени и удаленной идентификации, такие как распознавание лиц.

Запрет применяется с учетом сферы действия регламента, обозначенной в ст. 2. AI Act.

Уровень 2. Высокий риск

Системы ИИ, которые негативно влияют на безопасность или основные права, делятся на две категории:

1. Системы ИИ, которые используются в продуктах, подпадающих под действие законодательства ЕС о безопасности продукции.

2. Системы ИИ, относящиеся к восьми областям, перечислены в Приложении III AI Act.

Уровень 3. Малый риск

К ИИ малой степени риска отнесены специализированные реализации моделей ИИ, выход которых «имеет незначительное или подчиненное влияние на решения и действия человека», например, это системы ИИ, которые генерируют изображения, аудио- или видеоконтент. Для них регулирование сравнительно мягкое, такие приложения ИИ должны соответствовать минимальным требованиям прозрачности, которые позволили бы пользователям принимать обоснованные решения. Пользователи должны быть осведомлены, когда они взаимодействуют с ИИ. Приложения ИИ этой группы в настоящей статье не рассматриваются.

Генеративный искусственный интеллект (базовые модели)

В регламенте отдельно выделены базовые модели или генеративный ИИ (модели ИИ типа GPT-4, применяющиеся в областях типа медицины, управления транспортными средствами и пр.), которые могут относиться к любой группе риска.

Автономные системы ИИ (далее – АС) также могут относиться к любой группе риска. Согласно версии, предложенной Европейским парламентом и оставленной без изменения Советом Европейского союза, может быть отнесена к системам высокого риска, если она создает риск причинения вреда здоровью и безопасности или риск неблагоприятного воздействия на основные права, который эквивалентен или превышает риск причинения вреда, создаваемый системами ИС высокого риска и действует в одной из восьми сфер, отнесенных к Приложению III 2 (b) ст. 7 AI Act. AI Act не наделяет АС какими-либо особенностями по сравнению с приложениями ИИ, действующими на основе несамообучающихся моделей. Соответственно, ответственность лиц, контролирующих АС, не дифференцируется по сравнению с неавтономными приложениями АС. Это логично, поскольку полной автономии согласно регламенту, не предполагается: пользователи долж-

ны поручить человеческий надзор физическим лицам, обладающим необходимой компетенцией, обучением и полномочиями (п. 1a ст. 29 Council Mandate).

Итак, AI Act классифицирует системы ИИ на основе вероятности причинения ими вреда (ущерба), при этом большая часть регламента посвящена регулированию прав и обязанностей участников жизненного цикла систем ИИ высокого риска.

Рассмотрим, каков с точки зрения AI Act жизненный цикл приложения ИИ, каковы его основные участники.

3. Участники жизненного цикла приложений ИИ в регламенте ЕС AI Act

Согласно п. 1a ст. 3 AI Act (Council Mandate), «жизненный цикл системы ИИ» означает продолжительность работы системы ИИ от проектирования до выхода из эксплуатации (отключение без возможности дальнейшего использования или существенной модификацией системы ИИ).

Права и обязанности участников жизненного цикла приложений ИИ и, соответственно, ответственность за их несоблюдение (далее по тексту также «правовой режим») зависят от уровня риска, к которому относится система ИИ. Участниками жизненного цикла приложений, как представляется, являются поставщик, пользователь, производитель продукции, разработчик.

Поставщик (provider) – это любое лицо, включая государственный орган, который разрабатывает систему ИИ или у которого есть система ИИ, разработанная с целью ее размещения, и кто выводит эту систему на рынок или вводит ее в эксплуатацию под своим собственным именем или торговой маркой, будь то за плату или бесплатно (п. 2 ст. 3 AI Act).

Отдельно выделена конструкция «малый поставщик» – микро- или малое предприятие, что означает дифференцию правовых режимов поставщиков систем ИИ в зависимости от их размера. Поставщика не следует путать с разработчиком, правовой режим которого совершенно иной (см. ниже).

Поставщик базовой модели. Ст. 3 AI Act не дает определения поставщика базовой модели. Правовой режим поставщика базовой модели, обязанности которого перечислены в ст. 28b, добавленной в EP Mandate, отличается от правового режима поставщика, обязанности которого закреплены в ст. 16 AI Act. Примечательно, что из п. 2 ст. 28 AI Act в редакции EP и Council Mandate исчезло первоначальное предложение о том, что поставщик, который первоначально разместил систему ИИ с высоким уровнем риска на рынке или ввел ее в эксплуатацию, больше не считается поставщиком для целей AI Act. Анализ ст. 28b (EP Mandate) а также других положений AI Act позволяет прийти к выводу, что поставщик базовой модели – это лицо, разместившее на рынке универсальную модель машинного обучения, которая может быть адаптирована под широкий круг задач. Несмотря на кажущееся сходство, не следует путать поставщика базовой модели с разработчиком вообще и разработчиком базовой модели в частности.

Разработчик. Ст. 3 регламента не содержит определение понятия «разработчик». В первоначальном проекте регламента (Commission Proposal) разработчик не упоминается вовсе, однако его фигура появляется в п. 12c преамбулы EP Mandate, где говорится, что разработчики бесплатных компонентов ИИ с от-

крытым исходным кодом не должны быть обязаны соответствовать требованиям регламента в части регулирования цепочки создания стоимости ИИ, и в частности, требованиям, установленным в отношении поставщика, который использовал этот бесплатный компонент ИИ с открытым исходным кодом. Однако разработчиков бесплатных компонентов ИИ с открытым исходным кодом следует поощрять к внедрению широко распространенных методов документирования. Согласно абз. «o» ст. 56 b EP Mandate Офис ИИ (The European Artificial Intelligence Office) должен обеспечить мониторинг базовых моделей и организовать регулярный диалог с разработчиками базовых моделей на предмет их соответствия требованиям безопасности. Данные положения не изменены в Council Mandate. Соответственно, в случае вступления AI Act в силу к категории разработчиков будут относиться только разработчики бесплатных компонентов ИИ с открытым исходным кодом, а разработчики базовых моделей попадут в поле зрения государственного органа (Офис ИИ), который будет проверять действия таких разработчиков на соответствие регламенту.

Так, в отличие от поставщика базовой модели, разработчик базовой модели не выводит ее на рынок за плату или по бесплатным лицензиям с открытым исходным кодом, он может использовать базовую модель только в той мере, в которой такое использование не подпадает под действие регламента, например, в личных, научно-исследовательских целях.

Пользователь (user) означает любое лицо, включая государственный орган, использующий систему ИИ, находящуюся в его ведении («under whose authority»), за исключением случаев, когда система ИИ используется в ходе личной непрофессиональной деятельности (п. 4 ст. 3 AI Act). Для облегчения понимания функций пользователя следует упомянуть, что в редакции EP Mandate это же лицо обозначалось как деплоер (deployer), что в переводе на русский язык означает «разработчик» или «развертыватель». Это лицо, осуществляющее развертывание и запуск приложения ИИ. Однако в Council Mandate в этом же значении снова употребляется термин «пользователь», в роли которого может выступать любое лицо, использующее систему ИИ. Можно ожидать, что в финальной версии AI Act термин «deployer» окончательно уступит место термину «user». В целях настоящей статьи будем употреблять термин «развертыватель» в значении «пользователь» как синоним, тем более, что перевод слова «deployer» на русский язык – «развертыватель», не имеет общеупотребительного значения.

Следует согласиться с тем, что «любая организация, банки и даже супермаркеты могут квалифицироваться как пользователи в соответствии с предстоящим регламентом, если они хотят внедрить системы ИИ с высоким уровнем риска» [2].

Производитель означает производителя по смыслу любого законодательства ЕС о гармонизации, перечисленного в Приложении II. Соответственно, устанавливая правовые режимы, AI Act различает фигуры поставщика и производителя системы ИИ (п. 5a ст. 3 AI Act). Поскольку законодательство ЕС гармонизирует обязательные требования к безопасности продукции на всей территории ЕС, производитель обязан соблюдать указанные требования. По всей видимости, AI Act будет являться специальным нормативно-правовым актом по отношению к зако-

нодательству ЕС о гармонизации обязательных требований к безопасности продукции, в которой содержатся приложения ИИ.

Оператор означает поставщика, производителя продукции, пользователя, уполномоченного представителя, импортера и/или дистрибьютора (п. 8 ст. 3 AI Act). Термин «оператор» объединяет всех лиц, которые контролируют систему ИИ.

Представляется, что основными участниками жизненного цикла приложений ИИ в AI Act являются поставщик, разработчик базовых моделей и пользователь. Все они могут совпадать в одном лице, но чаще это разные организации.

Размер настоящего доклада не позволяет уделить внимание другим операторам.

4. Правовой режим основных участников жизненного цикла приложений ИИ в регламенте ЕС «AI Act»

Рассмотрим правовой режим основных участников жизненного цикла приложений ИИ, закрепленный в регламенте ЕС «AI Act», поскольку бремя ответственности за неблагоприятные последствия использования приложений ИИ должно распределяться между участниками соответственно их обязанностям.

В докладе анализируется только правовой режим систем ИИ высокого риска.

Поставщик

Список обязанностей поставщика систем высокого риска закреплен в ст. 16 AI Act, хотя три фундаментальные обязанности закреплены уже в преамбуле регламента в редакции Council Mandate.

Первая обязанность, которая лежит на поставщике (п. 32a преамбулы AI Act) – классификация приложений ИИ по уровню риска, которое он намерен вывести на рынок. Если оказывается, что приложение ИИ соответствует признакам систем высокого риска, то поставщик должен оценить, не представляет ли указанная система ИИ значительный риск причинения вреда здоровью, безопасности, основным правам или окружающей среде. До вывода на рынок, в идеале на стадии разработки, поставщик направляет в компетентный орган соответствующее уведомление. Если компетентный орган считает, что рассматриваемая система ИИ была неправильно классифицирована поставщиком, она должна быть отозвана с рынка. Корреспондирующая обязанность закреплена в п. «e» ст. 16 AI Act (Council Mandate).

Вторая обязанность поставщика (п. 42 преамбулы AI Act) –установление системы управления рисками, которая в соответствии с требованиями главы 2 AI Act представляет собой непрерывный процесс, реализуемый на протяжении всего жизненного цикла системы ИИ. Этот процесс должен гарантировать, что поставщик услуг идентифицирует и анализирует риски для здоровья, безопасности и основных прав лиц, которые могут быть затронуты системой ИИ в свете ее предполагаемого назначения, включая возможные риски, возникающие в результате взаимодействия между системой ИИ и средой, в которой она функционирует, и, соответственно, принимает соответствующие меры по управлению рисками в свете современного уровня техники.

Третья обязанность поставщика (п. 78 преамбулы AI Act) – иметь систему постпродажного мониторинга по месту использования для обеспечения своевременного устранения возможных рисков, связанных с системами ИИ, которые продолжают «обучаться» после выхода на рынок или ввода в эксплуатацию. Поставщики услуг также обязаны иметь действующую систему для сообщения соответствующим органам о любых серьезных инцидентах или любых нарушениях национального законодательства ЕС, защищающих основные права в результате использования их систем ИИ. Корреспондирующие обязанности закреплены в п. «g» и «h» ст. 16 AI Act (Council Mandate)).

Перечислим некоторые обязанности поставщика согласно ст. 16 AI Act, а именно, поставщики должны:

– обеспечивать соответствие их приложений ИИ требованиям, изложенным в главе 2 AI Act (п. «a» ст. 16 AI Act (Council Mandate)), в том числе, проходить процедуру оценки рисков в соответствии со 43 AI Act;

– уведомлять физических лиц, которым поручен человеческий надзор за системами ИИ, о риске автоматизации или предвзятости подтверждения (п. «ab» ст. 16 AI Act (EP Mandate, подтверждено Council Mandate)), чему корреспондирует обязанность пользователя использовать систему ИИ в соответствии с инструкцией, подготовленной поставщиком, включая осуществление мер по надзору за персоналом в целях осуществления человеческого контроля за ИИ (ст. 29 AI Act);

– предоставить информацию об используемых наборах входных данных (п. «ac» ст. 16 AI Act (EP Mandate, подтверждено Council Mandate));

– вести документацию (п. «c» ст. 16 AI Act (Council Mandate)) и журналы, автоматически генерируемые системами ИИ, находящимися под их контролем (п. «d» ст. 16 AI Act (Council Mandate));

– регистрировать системы ИИ высокого риска.

Согласно п. 1 ст. 43 AI Act поставщик должен выполнить одну из следующих процедур: (a) процедуру оценки соответствия, основанную на внутреннем контроле или (b) процедуру оценки соответствия, основанную на оценке системы менеджмента качества и технической документации с привлечением нотифицированного органа.

Следовательно, основная обязанность поставщика – это оценка и управление рисками в течение всего жизненного цикла системы ИИ, направленные на безопасность системы вплоть до ее отключения. Оценка и управление рисками включают в себя, прежде всего, техническое документирование разработки и подготовку подробных инструкций для пользователя. Иные обязанности (например, пострыночный, сообщение об инцидентах и пр.), как представляется, либо направлены на удаление из хозяйственного оборота опасных приложений ИИ, либо на улучшение качества приложений ИИ, включая уточнение инструкций.

Поставщик базовой модели (provider of foundation model)

Понятие базовой модели в Commission Proposal отсутствовало и появилось в ходе законодательного процесса: EP Mandate добавил определение понятия базовой модели в ст. 3, а также закрепил обязательства поставщика базовой модели в ст. 28b.

Согласно п. 1 «c» ст. 3 AI Act (EP Mandate), базовая модель означает модель системы ИИ, которая обучается на обширных данных в масштабе (broad data at scale), предназначена для обобщения выходных данных и может быть адаптирована к широкому спектру задач.

Иными словами, это универсальная предобученная модель машинного обучения. Наиболее известны модели вида GPT, но ими круг базовых моделей не ограничивается.

Согласно п. 1 ст. 28b AI Act (EP Mandate), поставщик базовой модели должен до вывода на рынок или ввода в эксплуатацию убедиться, что она соответствует требованиям, изложенным в ст. 28b, независимо от вида приложения, в которое она встроена, и возмездности распространения (платно или на условиях свободной лицензии). Эти требования закреплены в п. 2 ст. 28b, из которых ключевыми являются обязанности:

(a) предвидеть и оценивать последствия разработки для человека и окружающей среды, контролировать качество данных;

(b) обучать модель только на данных, которые подлежат эффективному контролю на протяжении всего своего жизненного цикла;

(c) спроектировать и обучить базовую модель так, чтобы на протяжении всего ее жизненного цикла она была безопасной и (d) отвечала требованиям соответствующих стандартов;

(e) разработать техническую документацию и понятные инструкции по использованию, с тем чтобы дать возможность нижестоящим поставщикам выполнять свои обязательства в соответствии со статьями 16 и 28(1) регламента;

(f) создать систему менеджмента качества для обеспечения и документирования соответствия модели требованиям ст. 28b AI Act;

(g) зарегистрировать базовую модель в базе данных ЕС.

Законодатель не ссылается на главу 2 AI Act, где установлены требования к системам ИИ высокого риска не случайно. Это обусловлено в первую очередь тем, что базовая модель – это программа для ЭВМ, а глава 2 регулирует обязанности поставщиков систем ИИ, которые могут быть программно-аппаратными комплексами (т. е. устройствами), в которых могут быть использованы (но далеко не всегда) базовые модели AI Act и которые доводятся до пользователей и потребителей, поэтому к программе для ЭВМ круг требований сужен обязанностями, перечисленными в ст. 28b.

По сути, ст. 28b AI Act устанавливает требование к системе управления рисками с упором на контроль качества данных и документирование, направленные на обеспечение адекватности и безопасности системы ИИ на самом вышестоящем уровне, где нижестоящий поставщик использует базовую модель вышестоящего поставщика.

Следовательно, основная обязанность поставщика базовой модели – спланированная безопасность модели, которая достигается контролем качества обучающих данных в течение всего ее жизненного цикла.

Пользователь

В п. 58a Преамбулы AI Act в редакции EP Mandate (без последующих изменений в Council Mandate) указывается на то, что «риски, связанные с системами ИИ, могут проистекать не только из способа проектирования таких систем, но и из того, как такие системы ИИ используются. Таким образом, развертыватели (deployers) систем ИИ играют важную роль в обеспечении защиты основных прав, дополняя обязательства поставщика при разработке системы ИИ». В этой фразе достаточно однозначно выражено отношение европейского законодателя к обязательствам пользователя в обеспечении предотвращения вреда (ущерба) от использования систем ИИ – как дополнительным по отношению к обязательствам поставщика. Означает ли это субсидиарную ответственность за вред (ущерб)? Думается, что нет – это работает иначе. Поскольку, согласно п. 1 ст. 29 AI Act, пользователь должен использовать систему ИИ в соответствии с инструкцией, предоставляемой поставщиком, при этом контролировать систему должно только компетентное физическое лицо (п. 1a ст. 29 AI Act (Council Mandate)). Соответственно, если пользователь действует в строгом соответствии с инструкцией, а инцидент все же случается, то за неблагоприятные последствия инцидента должен отвечать поставщик. Однако не все так однозначно: AI Act учитывает действия пользователя.

В этом же п. 58a Преамбулы далее указано, что пользователи лучше всего понимают, как конкретно будет использоваться система ИИ, и, следовательно, могут идентифицировать потенциальные значительные риски, которые не были предусмотрены на этапе разработки, благодаря более точному знанию контекста использования, людей или групп людей, которые могут быть затронуты, включая уязвимые группы. Лица, осуществляющие развертывание (т. е. пользователи), должны определить соответствующие структуры управления в данном конкретном контексте использования, такие как механизмы надзора за персоналом, процедуры рассмотрения жалоб и процедуры возмещения ущерба. Пользователь систем ИИ должен проводить оценку воздействия на основные права до ввода их в эксплуатацию и выполнять ряд связанных с этим обязанностей (детали определены в ст. 29(a) AI Act (EP Mandate)), что требует огромных человеческих усилий и возможностей, поэтому, согласно регламенту (58a Преамбулы, EP), эти обязательства не должны распространяться на малые и средние предприятия, которые тем не менее также должны стремиться к проведению вышеуказанной оценки. Если обнаруженные риски не могут быть уменьшены, пользователи должны вообще воздерживаться от использования такой системы ИИ. Положительным моментом для пользователей является то, что они смогут воспользоваться существующими оценками, проводимыми поставщиками, в той мере, в какой предоставляемая оценка включает минимальные элементы, определенные AI Act. Это правило в значительной степени перекидывает обязанность по оценке рисков (а следовательно, и ответственность за инциденты) обратно на поставщика. Учитывая то, что у большинства коммерческих компаний нет необходимых источников для проведения оценки воздействия на основные права человека, неясно, как на практике будет реализовываться данное требование: вполне возможно, что очень формально и бессмысленно для защиты прав человека, но весьма обременительно как для постав-

щика, так и для пользователя. Не исключено, что на практике пользователи будут избегать обязанности по оценке или проводить ее формально, целиком полагаясь на документы (по оценке, инструкции и пр.), предоставляемые поставщиком.

Правило AI Act ((58a), EP Mandate), которое требует от пользователей в случае нарушения прав какой-либо группы лиц сообщать о результатах оценки воздействия системы ИИ на основные права национальным надзорным органам и производить общедоступную публикацию отчета об оценке (видимо, без разглашения сведений о затронутых физических лицах), напоминает требование об уведомлениях в связи с утечкой данных, но вряд ли будет эффективно работать, потому что содержит оценочное суждение «о результатах оценки воздействия системы ИИ на основные права», которое может оказаться необъективным, так как критерии оценки не разработаны.

Согласно п. 6 ст. 29 AI Act требуется, чтобы пользователи проводили оценку воздействия на защиту данных (далее «data protection impact assessment» будет обозначена как «DPIA») в соответствии с требованиями GDPR применительно к ситуации, когда персональные данные обрабатываются на протяжении всего жизненного цикла системы ИИ. EP Mandate внес два дополнения. Отмечается, что эти новые обязательства заставят пользователей и контролеров данных активизировать свои усилия по обеспечению соответствия требованиям GDPR [2].

Государственные органы или организации широкого круга категорий, обязаны зарегистрировать факт использования любой системы ИИ с высоким уровнем риска в общедоступной базе данных. Другие участники развертывания могут зарегистрироваться добровольно.

Очевидно, что у пользователя так же, как и у поставщика, много обязанностей по обеспечению безопасности использования приложений ИИ, но эти обязанности в основном имеют «умозрительное содержание» могут быть исполнены лишь формально, тем самым ничего или почти ничего не добавляя к укреплению безопасности ИИ и защите прав человека.

Итак, мы рассмотрели права и обязанности основных участников жизненного цикла приложений ИИ. Что в соответствии с AI Act является нарушением, за которое полагается ответственность? Какая ответственность вытекает из обязанностей операторов систем ИИ и как она распределяется?

5. Административная ответственность участников жизненного цикла приложений ИИ за нарушение обязанностей согласно AI Act

AI Act предусматривает только административную ответственность за несоблюдение требований регламента. В ст. 71 перечислены штрафы операторов и других участников жизненного цикла систем ИИ, причем самые крупные санкции (30 000 000 EUR, а для МП – 6% от годового оборота по всему миру) предусмотрены за нарушение ст. 5 AI Act, где перечислены запрещенные практики использования ИИ. Также штрафы вводятся за следующие нарушения:

– обязательств поставщиков, установленные в ст. 16 AI Act;

– обязательств другими участниками жизненного цикла приложений ИИ (перечислены конкретные статьи, где установлены различные обязательства).

В ст. 72 AI Act перечислены штрафы, налагаемые на профсоюзные учреждения, агентства и ведомственные структуры – на государственные органы.

Распределение гражданско-правовой ответственности за вред, причиненный приложениями ИИ, AI Act напрямую не регулирует.

Однако, как представляется, AI Act регулирует распределение гражданско-правовой ответственности за вред (ущерб), причиненный приложениями ИИ косвенно.

Так, к примеру, AI Act вводит понятие серьезного инцидента. В соответствии со статьей п. 44 ст. 3 AI Act (Council Mandate) «серьезный инцидент» («serious incident») означает любой инцидент или сбой в работе системы ИИ, который прямо или косвенно приводит к любому из событий, перечисленных в п. 44 ст. 3.

В AI Act определены обязанности поставщика и пользователя по осуществлению человеческого надзора и контроля за работой системы ИИ и порядок действий в случае серьезного инцидента (напр., ст. 62 AI Act, Council Mandate для поставщика, ст. 65(1) AI Act, п. 4 ст. 29 AI Act, Council Mandate для пользователя). Исполнение или неисполнение этих обязанностей имеет значение для распределения гражданско-правовой ответственности.

6. Влияние положений AI Act на распределение гражданско-правовой ответственности за вред (ущерб), причиненный приложениями ИИ

По общему правилу, для установления состава гражданско-правового правонарушения истец должен доказать, что действия или бездействие ответчика причинили вред (ущерб). Для этого истец должен доказать, что причиненный вред был предсказуемым следствием поведения ответчика, однако в связи с появлением систем ИИ с их непрозрачными процессами вывода результата это правило работает неэффективно.

Поэтому Европейская комиссия разработала директиву об ответственности за ИИ [5], цель которой состоит в том, чтобы адаптировать деликтное право к отличительным особенностям несчастных случаев, вызванных системами ИИ, в частности, изменения касаются облегчения бремени доказывания наличия причинно-следственной связи между применением ИИ и неблагоприятными последствиями [1].

Директива об ответственности за ИИ вводит опровержимую презумпцию причинно-следственной связи между применением ИИ и причинением вреда (ущерба). Как отмечается в комментарии к директиве, в ней проводится ограниченная презумпция «связи между нарушением ответчиком обязанности проявлять осторожность и результатами работы системы ИИ». Так, поставщик может защититься от иска предъявлением доказательств установления у себя системы управления рисками, соответствующей требованиям главы 2 AI Act, и тем самым доказать надлежащее исполнение обязанности проявлять осторожность и должную осмотрительность. Дополнительно можно представить результаты пост-маркетингового мониторинга, дополненного статистикой отсутствия серьезных инцидентов. В этой связи возникает вопрос, кто будет нести ответственность за вред (ущерб) в случае надлежащего исполнения всех наложенных регламентом «AI Act» обязательств и поставщиком (включая поставщика базовой модели), и поль-

зователем, и другими участниками? На практике, вероятно, вопрос всегда будет разрешаться в чью-то пользу, поскольку вряд ли ответчикам удастся представить систему безупречного документирования. Однако если абстрагироваться и представить себе, что имеются идеальные документы, подтверждающие соблюдение всех требований AI Act, а вред (ущерб) все же причинен, т. е. впервые возник тот самый серьезный инцидент, то кто будет отвечать в этом случае?

В случае если при вышеописанных обстоятельствах вред (ущерб) причинен продуктом, в котором использовано приложение ИИ, то, согласно Пересмотренной PLD, наличие дефекта изделия и причинно-следственная связь между дефектом и вредом (ущербом) предполагаются. Согласно Пересмотренной PLD, также предлагается облегчить бремя доказывания, когда истец сталкивается с чрезмерными трудностями при доказательстве наличия дефекта и/или причинно-следственной связи между дефектом и повреждением из-за технической сложности продукта. Хотя в тексте Пересмотренной PLD конкретно не упоминаются системы ИИ и товары с использованием ИИ, Комиссия ЕС прямо определила, что эти продукты подпадают под действие этой презумпции.

Получается, что после принятия обеих директив и регламента в вышеуказанном случае, приведенном в качестве абстрактного примера, отвечать должен все-таки поставщик, даже при наличии у него системы идеального документирования, потому что есть опровержимая презумпция наличия причинно-следственной связи между дефектом и вредом (ущербом), причиненным продуктом, которая при определенных обстоятельствах освобождает от ответственности пользователя. Представляется, что опровергнуть эту презумпцию поставщик сможет далеко не всегда.

Заключение. Состязательный характер судебного процесса и презумпции можетт не обеспечивать в полной мере защиту основных прав человека, поэтому вполне логично принятие регламента «AI Act», направленного на предотвращение вреда (ущерба).

В целом AI Act направлен на регулирование правоотношений между операторами систем ИИ, основными из которых являются поставщик, поставщик базовых моделей и пользователь. AI Act защищает права потребителей опосредованно – через установление обязанностей операторов систем ИИ.

Согласно AI Act, наиболее широкий круг обязанностей по обеспечению безопасности приложений ИИ закреплен за поставщиком. У пользователя тоже достаточно обременительные обязанности. Однако если у поставщика обязанности по обеспечению безопасности ИИ вполне материальные, то у пользователя они представляются умозрительными по своей сути, поэтому их исполнение на практике легко может превратиться в «набор отписок», так как состоят эти обязанности в основном в документировании оценочных суждений.

Поэтому, как представляется, основное бремя обеспечения безопасности приложений ИИ и ответственность за причиненный им вред (ущерб) в ЕС ложится на поставщика, что последовательно проводится в регламенте «AI Act», Директиве об ответственности за ИИ и Директиве об ответственности за дефектную продукцию.

Учитывая то, что пользователь потенциально может уйти от ответственности даже за свое виновное поведение, предоставив доказательства проявления осторожности, заключающиеся, прежде всего, в документировании оценки воздействия использования системы ИИ на основные права человека, справедливый, по мнению законодателя, баланс распределения ответственности за вред (ущерб), причиненный приложениями ИИ, может быть легко нарушен несправедливым сдвигом бремени ответственности в сторону поставщика. Это не только способно затормозить развитие разработок в области ИИ, но и привести к существенному удорожанию приложений ИИ для пользователей, которым придется нести значительные расходы на перенос бремени ответственности на поставщика, мало что добавляя при этом к безопасности использования ИИ. Вместе эти два фактора способны снизить темпы развития ИИ в ЕС.

В свете AI Act особенно сомнительны перспективы развития автономных систем. Условие абз. «b» п.2 ст. 28b AI Act (EP Mandate), согласно которому поставщик базовой модели обязан обучать модель только на данных, которые подлежат эффективному контролю на протяжении всего своего жизненного цикла, представляется практически невыполнимым для самообучающихся моделей, в связи с чем буквальное выполнение данного условия способно привести к невозможности коммерциализации моделей, обучающихся автономно. В дополнение к иным требованиям, предъявляемым регламентом, вряд ли у поставщиков базовых моделей останутся стимулы для работы там, где применяется AI Act. Впрочем, так же как и у поставщиков приложений ИИ, а вслед за ними и у других операторов.

Список литературы

1. Amrita Vasudevan, A. Who Is Liable for AI-Driven Accidents? The Law Is Still Emerging to establish negligence, a plaintiff needs to prove causation. 06.2023. URL: https://www.cigionline.org

2. Demircan M. Deployers of High-Risk AI Systems: What Will Be Your Obligations Under the EU AI Act? LSTS Research Group, Vrije Universiteit Brussel). June 2, 2023. URL: https://competitionlawblog.kluwercompetitionlaw.com

3. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. URL: https://eur-lex.europa.eu

4. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. 2021/0106(COD). DRAFT. 20-06-2023 at 16h53. URL: https://www.europarl.europa.eu

5. Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive). URL: https://commission.europa.eu

6. Proposal for a directive of the European Parliament and of the Council on liability for defective products. URL: https://eur-lex.europa.eu

В. Д. Полухина,
аспирант,
Новосибирский университет экономики и управления

ЦИФРОВОЕ ДИПЛОМАТИЧЕСКОЕ ИСКУССТВО: РОЛЬ ТЕХНОЛОГИЙ В СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

Аннотация. В статье рассматривается влияние цифрового дипломатического искусства на современные международные отношения. Дается анализ эволюции дипломатии в эпоху цифровых технологий, включая использование виртуальных конференций и социальных сетей. Исследуется роль цифровых платформ в формировании общественного мнения, в информационной войне в международной политике. Отмечаются перспективы и вызовы, возникшие перед современной дипломатией в цифровую эпоху, и подчеркивается важность исследования для дипломатов и ученых в области международных отношений и цифровой трансформации.

Ключевые слова: цифровая трансформация, международные отношения, кибербезопасность, киберпространство, современные технологии, информационная война, публичная дипломатия

DIGITAL DIPLOMATIC ART: THE ROLE OF TECHNOLOGY IN MODERN INTERNATIONAL RELATIONS

Abstract. This article examines the influence of digital diplomatic art on modern international relations. She analyzes the evolution of diplomacy in the digital age, including the use of virtual conferences and social networks. The article also explores the role of digital platforms in shaping public opinion and information warfare in international politics. The article puts forward the prospects and challenges facing modern diplomacy in the digital age, and emphasizes the importance of this research for diplomats and researchers in the field of international relations and digital transformation.

Keywords: digital transformation, international relations, cybersecurity, cyberspace, modern technologies, information warfare, public diplomacy

В современном мире цифровая трансформация оказала значительное воздействие на различные сферы жизни общества. Мировая политика отражает эти тенденции, переживая динамику и вызовы в этой области. Цифровой трансформацией можно назвать процесс интеграции и использования современных информационных и коммуникационных технологий, таких как Интернет, цифровые платформы, биг-дата – анализ, искусственный интеллект и другие, для преобразования различных областей общества и экономики. Этот процесс включает в себя цифровизацию производства, цифровую дипломатию, кибербезопасность и многие направления, связанные с использованием цифровых технологий.

Цифровая трансформация изменила скорость и доступ к информации: сделала его практически мгновенным и широкодоступным, что позволило гражданам и организациям быстро распространять новости и мнения о них. Данное явление привело к увеличению активности общества и возникновению новых возможностей для гражданской активности, таких как массовые протесты и движения [4].

Вместе с этим публичная дипломатия получила новый виток развития. Политические лидеры и правительства стали активно использовать социальные сети для общения с гражданами и представителями других стран. Это сделало возможным осуществление публичной дипломатии непосредственно через цифровые каналы, что размыло традиционные границы между внутренней и внешней политикой.

Подобный всеобщий доступ несет в себе не только положительные моменты – возможность представителей власти проводить активнее свою политику, но имеет следствием протестные движения в обществе. Таким образом, цифровые технологии стали инструментом информационных войн и манипуляции общественным мнением. Государства и негосударственные акторы используют дезинформацию и «фейки» для достижения своих целей, для воздействия на политические процессы в других странах.

Существенным вызовом современности при ускорении темпов цифровизации является вопрос кибербезопасности. Увеличение зависимости от цифровых систем создало новые угрозы в виде кибератак и кибершпионажа. Это привело к усилению внимания к вопросам кибербезопасности на мировой арене и к разработке международных соглашений в этой области.

Цифровая трансформация мира вынуждает мировое сообщество применять новые методы и подходы к дипломатической деятельности, в том числе разработку и подписание новых соглашений и конвенций в этой области. Рассматриваются документы по использованию цифровых инструментов в проведении международных переговоров и дипломатических усилий: такие как Будапештская конвенция 2001 года [3. С. 12], являющаяся самым первым договором в области преступлений, совершенных через Интернет. В ней устанавливаются обязательства для государств-участников по наказанию лиц, совершивших киберпреступления, и содействию в расследовании. Принимаются документы о принципах поведения государств в киберпространстве. Организация по безопасности и сотрудничеству в Европе (ОБСЕ) разработала набор принципов поведения государств в киберпространстве и призывает к сотрудничеству, доверию и соблюдению международных норм в этой области [7. С. 32].

Киберпространство является относительно новой и быстро развивающейся областью, в связи с чем международные соглашения и конвенции в этой сфере все еще разрабатываются и согласовываются. Однако существуют несколько важных международных инициатив и договоренностей в области киберпространства. Соглашение ЕС – США о защите персональных данных [6. С. 1]. Хотя это Соглашение не ограничивается исключительно киберпространством, оно регулирует передачу и обработку персональных данных между Европейским сою-

зом и Соединенными Штатами. Это имеет отношение к вопросам приватности и кибербезопасности.

Соглашение о создании цифрового мира [10. С. 82], представленное Китаем, нацелено на создание международного фонда для кибербезопасности и содействия общей безопасности в киберпространстве.

Приведенные примеры демонстрируют разнообразие инициатив и соглашений, разрабатываемых международным сообществом в области кибербезопасности. Важно отметить, что эта область продолжает развиваться, и новые направления деятельности могут возникнуть в будущем для более эффективного управления киберпространством. Несмотря на эти и другие международные инициативы, многие вопросы в области кибербезопасности остаются сложными и представляют вызов для глобального сообщества. Регулирование кибербезопасности в мировых отношениях остается активной областью дипломатической деятельности и исследования [5. С. 10].

Рассматривая вопрос о роли современных технологий в международных отношениях, нельзя не затронуть вопрос глобальной экономики. Быстрое распространение технологий изменило и экономические структуры, создало новые формы экономической деятельности, такие как цифровые платформы и криптовалюты [8. С. 337]. Это вызвало дискуссии о регулировании и налогообложении в глобальной экономике [13. С. 4].

Отдельной уникальной темой для обсуждения вопроса регулирования и построения механизмов безопасности выступает искусственный интеллект. Уже сейчас вполне очевидно, что ИИ даже в текущей реализации может стать универсальным инструментом для совершения киберпреступлений [11. С. 79]. ИИ может представлять угрозу для безопасности государства в цифровой среде по ряду причин [12]. Он может использоваться злоумышленниками для проведения кибератак, создания фейковых новостей и манипуляции информацией, разработки автоматизированных систем оружия, нарушения приватности и незаконного доступа к данным, а также для проведения социальной инженерии [5. С. 10]. Все это подчеркивает необходимость разработки строгих правил и этических стандартов в области использования ИИ, а также усиление кибербезопасности и защиты от кибератак [1. С. 2].

Борьба с угрозами со стороны ИИ требует комплексного подхода, который включает в себя разработку строгих правил и этических стандартов, усиление кибербезопасности, сотрудничество и обмен информацией, обучение и осведомленность людей, а также разработку новых технологий [2. С. 2]. Это сложная задача, но совместные усилия государств, организаций и общества помогут справиться с этими угрозами и обеспечить безопасность в цифровой среде [9. С. 23].

В целом, цифровая революция стала ключевым фактором в изменении динамики мировой политики, создав новые возможности и вызовы для государств и международных акторов. Это требует постоянного адаптивного подхода и разработки новых стратегий в мировой политике.

Список литературы

1. Brynjolsson E. “Machine learning will be the engine of global growth” // Opinion, Financial Times. 2018. July 26.

2. CHEN S. Artificial intelligence, immune to fear or favor, is helping to make China’s foreign policy // South China Morning Post. 2018. July 13. https://m.scmp.com/news/china/society/article/2157223/artificial-intelligence-immune-fear-or-favourhelping-make-chinas

3. Convention on Cybercrime by 23.06.2001 // Council of Europe. 2001.

4. Orr T. The Information Revolution: Transforming the World Through Technology. New York: Lucent Press, 2020. URL: http://search.ebscohost.com/login.aspx?direct=true&site=eds-live&db=edsebk&AN=2174025

5. Гришанина Т. А. Искусственный интеллект в международных отношениях: роль и направления исследования // Вестник РГГУ. Серия Политология. История. Международные отношения. 2021. № 4. С. 10-18.

6. Евросоюз принял третье соглашение с США о безопасном экспорте личных данных, но и его, возможно, придется переделывать. URL: https://3dnews.ru/1089725/evrosoyuz-prinyal-trete-soglashenie-ob-eksporte-personalnih-dannih-v-ssha-no-kritiki-popregnemu-schitayut-ego-nedorabotannim

7. Ежегодный доклад ОБСЕ. URL: https://www.osce.org/files/f/documents/c/4/91840.pdf

8. Лексин В. Н. Искусственный интеллект в экономике, политике и частной жизни: Опыт системной диагностики. М.: Ленанд, 2021. 336 с.

9. Румате Ф. Искусственный интеллект и международные отношения: новый баланс сил в новом мировом порядке // Коммуникации. Медиа. Дизайн. 2022. № 7(1). С. 23-33.

10. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики о сотрудничестве в области обеспечения международной информационной безопасности от 8 мая 2015 г. // Бюллетень международных договоров. 2016. № 11. С. 82-88.

11. Солодов Д. А., Шиверов П. К., Иванова П. Н. Искусственный интеллект в международных отношениях и дипломатической службе // Вестник Дипломатической академии МИД России. Россия и мир. 2020. № 4(26). С. 79-94. EDN ILYSVM

12. Бегишев И. Р., Хисамова З. И. Искусственный интеллект и уголовный закон. Москва: Проспект, 2021. 192 с. EDN DZCJKJ

13. Шелепов А. В. Влияние политики лидеров цифровизации - членов «группы двадцати» на механизмы международного регулирования и условия развития цифровой экономики // Вестник международных организаций: образование, наука, новая экономика. 2022. № 1.

В. Б. Романенко,
кандидат юридических наук, доцент,
Всероссийский государственный университет юстиции
(РПА Минюста России)
Ростовский институт (филиал)

ПРАВО НА ДОСТУП В ИНТЕРНЕТ В РАМКАХ ПРАВ ПЕРВОГО ПОКОЛЕНИЯ: МЕЖДУНАРОДНО-ПРАВОВОЙ АСПЕКТ

Аннотация. В статье рассматриваются проблемы прав человека в цифровую эпоху, в частности, акцент делается на особенностях реализации права на доступ в Интернет в контексте прав первого поколения путем использования информационно-телекоммуникационных технологий, стремительно развивающихся в последнее время. Автор анализирует международно-правовое и национальное законодательство некоторых стран, оказавшихся в авангарде закрепления и регулирования права на доступ в Интернет.

Ключевые слова: права человека, право на доступ в Интернет, цифровые права, цифровые технологии, государства, международно-правовые акты

RIGHT TO ACCESS TO THE INTERNET WITHIN THE FRAMEWORK OF FIRST GENERATION RIGHTS: INTERNATIONAL LEGAL ASPECT

Abstract. The article examines the problems of human rights in the digital age, in particular, the emphasis is on the specifics of implementing the right to access the Internet in the context of first-generation rights through the use of information and telecommunication technologies, which have been rapidly developing in recent times. The author analyzes the international legal and national legislation of some countries that have been at the forefront of securing and regulating the right to Internet access.

Keywords: human rights, right to access the Internet, digital rights, digital technologies, states, international legal acts

Стремительное развитие информационно-телекоммуникационных технологий в последние годы привело к тому, что сейчас Интернет перестал быть только средством хранения и распространения информации. Цифровизация затрагивает практически все сферы жизнедеятельности человека, что требует переосмысления многих фундаментальных юридических понятий. Одним из них являются права человека. Сегодня все чаще утверждается, что технологические инновации влекут за собой появление новых цифровых прав человека, которые принципиальным образом отличаются от традиционных и образуют новое поколение прав человека. Наиболее часто среди таких прав называют право на доступ к Интернету, право на защиту персональных данных и право на забвение (право на удаление). Однако следует различать «право на Интернет» и реализацию прав через Интернет.

Прежде всего необходимо ответить на вопрос о том, чем является «право на Интернет», каково его правовое регулирование. Оно не урегулировано такими общепризнанными международными инструментами, как Всеобщая декларация

прав человека, международные пакты и иные документы (время Интернета пришло позже их принятия).

В то же время, говоря о «праве на Интернет» и принципе равенства прав и свобод, нужно учитывать, что это право зависит, кроме всего прочего, и от уровня экономического развития страны в целом, от уровня развития в государстве информационно-коммуникационных технологий, от открытости Интернета, от возможностей самого человека. Таким образом, не всякий человек может реализовать «право на Интернет». А там, где реализация права доступна, государство может ввести ограничения, включая цензуру, или условия для получения какой-либо информации, например, только при предоставлении личных сведений, и т. д.

В частности, в Китае новые технологии применяются для обеспечения безопасности интересов собственной страны и ее граждан за счет введения тотального контроля за действиями граждан, формирования своеобразного интернет-паспорта каждого гражданина, установления связи между предоставлением прав и реализацией обязанностей, проявлением политических настроений конкретного лица. Вряд ли можно говорить о сохранении гарантий реализации прав граждан в такой ситуации, скорее, государство серьезно ограничивает реализацию прав человека.

В Египте летом 2018 г. для обеспечения национальной безопасности был принят Закон «О борьбе с киберпреступностью», ужесточающий контроль властей за Интернетом.

В Индии в 2007 г. был принят Акт об информационных технологиях. Была введена частичная цензура. Поводом явились террористические акты в Мумбаи, поэтому ограничения коснулись прежде всего политических и экстремистских ресурсов.

Блокируются отдельные сайты и в Пакистане. Поводом здесь обычно служат этносепаратистские материалы. Подчас поводы для введения ограничений дают и иные события. Например, в Японии ограничение было введено после землетрясения и аварии на АЭС «Фукусима», чтобы прекратить распространение информации о последствиях аварии.

Однако самый первый закон о введении цензуры в Интернете был принят еще в 1995 г. в Южной Корее (особые ограничения касались сочувственных высказываний о Северной Корее). В самой Северной Корее ограничения обеспечиваются прежде всего запретом на беспроводные сети и контролем за самими компьютерами.

Интересен опыт доступа в Интернет Эстонии, которая является одним из примеров системного применения информационных технологийдля реализации прав человека.

И, хотя Конституция Эстонии не содержит каких-либо гарантий относительно информационных технологий, тем не менее закреплены многичисленные достижения в данной области. Так, в частности, отмечается высокий уровень доступа населения к информационным магистралям, благодаря государственной политике в сфере компьютеризации, проведенной в 1996 г. Кроме того, законодательно закреплена возможность для каждого человека получить доступ к общественной информации через Интернет в публичных библиотеках. Необходимо

отметить также, что Эстония – первая страна в мире, которая стала выстраивать систему электронного правительства, развивала электронный документооборот, обеспечивала министрам возможность принимать участие в работе правительства дистанционно и др.

Еще одной страной с интересным опытом в отношении права на Интеренет является Непал, где существует конституционное закрепление права на доступ в Интеренет. Кроме того, законодательство Непала подробно регулирует проведение коммерческих и финансовых транзакций, а также некоторые важные аспекты, касающиеся ограничения ответственности провайдера за различные нарушения функционирования электронных коммуникаций и безопасности информации.

В отдельных государствах (Азербайджан, Бразилия, Венесуэла, Индия, Колумбия, Кыргызстан, Ливия, Мексика, Нигерия, Сингапур, Тунис, Украина, Южная Корея и др.) Интернет ограничен частично. В Беларуси, Египте, Иране, Казахстане, Китае, Кубе, России, Турции, ОАЭ и некоторых других странах установлены довольно жесткие ограничения в отношении использования интернет-пространства [1. С. 7].

Для понимания права на Интернет важно определить его содержание, а также содержание прав, которые реализуются в Сети. Впервые международное признание права на доступ к Интернету получило упоминание в Докладе Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Рю от 16 мая 2011 г. (A/HRC/17/27) [2], который был представлен Совету по правам человека ООН в соответствии с его Резолюцией 7/36 от 28 марта 2008 г. [3], где ему поручалось «продолжать излагать свои мнения о преимуществах и проблемах, обусловленных новыми информационными и коммуникационными технологиями, включая Интернет и мобильную связь». Доклад интересен тем, что в нем представлены и систематизированы различные аспекты обеспечения доступа к Интернету.

Кроме того, Интернет рассматривается в докладе в качестве «ключевого средства» реализации свободы выражения мнений, гарантированной ст. 19 Всеобщей декларации прав человека [4], которая «была составлена таким образом, чтобы охватить и учесть будущие технологические разработки», в связи с чем «принципы международного права прав человека остаются актуальными и по сей день и одинаково применимыми к новым коммуникационным технологиям, таким как Интернет». Собственно, в докладе речь и идет о мерах, необходимых для реализации свободы выражения и свободы информации в Интернете.

В документе выделяются два аспекта доступа к Интернету: свободный доступ к содержащемуся в нем контенту (включая его создание и размещение) и наличие для этого необходимой инфраструктуры и информационно-коммуникационных технологий, таких как кабели, модемы, компьютеры, программное обеспечение и т. п.

Право на доступ к Интернету своими корнями уходит к двум тесно взаимосвязанным правам первого поколения – свободе выражения и праву на информацию – и в общем может рассматриваться как средство их реализации.

В отношении прав первого поколения (свобода контента в Интернете) в докладе названы следующие негативные обязательства государств: недопустимость

произвольного блокирования или фильтрации контента, лишающего возможности получать и распространять информацию в Интернете, а также лишения доступа к Интернету (отключения от Интернета), в том числе при нарушении прав интеллектуальной собственности; запрет необоснованного нарушения конфиденциальности деятельности в Интернете (в том числе контроль переписки и иных сообщений) и криминализации законного выражения мнений в Интернете (отслеживания лиц, которые конфиденциально ищут, получают и передают информацию через Интернет, их задержание, содержание под стражей, иные формы преследования и запугивания). К числу позитивных обязательств государств, выводимых из содержания Доклада, можно отнести: борьбу с кибератаками, т. е. предоставление защиты от несанкционированного проникновения в учетные записи и компьютерные сети (выявление виновных и привлечение их к ответственности, принятие предупредительных мер); защиту персональных данных; регулирование деятельности частных корпораций-посредников, которые обеспечивают коммуникацию в Интернете (размещение, передачу, индексирование контента и предоставление к нему доступа), в том числе их ответственности за размещение незаконного пользовательского контента.

Однако, по мнению ученых, доклад не является свидетельством «очевидного международного признания интернет-прав», что из него следует необходимость «признания доступа к Интернету в качестве права человека» и что ООН признала «право на доступ к Интернету неотъемлемым правом человека» [5. С. 44], во-первых, в связи с сугубо рекомендательным характером этого документа, во-вторых, исходя из его содержания, в котором используются весьма осторожные формулировки, не дающие оснований для столь далеко идущих выводов.

Обоснование права на доступ к Интернету остается спорным вопросом и на доктринальном уровне. Ученые отмечают, что доступ к Интернету не может рассматриваться как универсальное естественное право, принадлежащее всем людям в силу их природы. Природа человека не предполагает доступа к Интернету, люди веками жили без него без ущерба для своей природы и, возможно, будут обходиться без него и в будущем, если на смену Интернету придут новые, более эффективные технологии [6. С. 6–8].

Необходимо учитывать еще один аспект. Доступ к Интернету сам по себе юридической ценности не имеет, он важен как средство реализации других прав и в целом свободы человека – основы всех его естественных прав. Социальные формы и способы бытия человеческой свободы разнообразны и исторически изменчивы. Сегодня они становятся все более технологически оснащенными и технологически зависимыми. Интернет (и необходимость доступа к нему) – одно из проявлений этой тенденции. Притязания на конкретные социально-исторически и культурно (в том числе и технологически) обусловленные способы реализации личной свободы вполне могут квалифицироваться как права человека. Безусловно, осуществление практически всех прав человека возможно (пока еще возможно) и без доступа к Интернету, но гораздо менее эффективно [7. С. 35].

И все же именно инструментально-технологическое понимание Интернета является основным препятствием к признанию доступа к нему самостоятельным

правом человека. Интернет рассматривается как исторически преходящий инструмент реализации различных прав, доступ к которому сам по себе правом быть не может: «...Лошадь, возможно, когда-то была незаменима для жизни человека, но теперь ей на смену пришли сто лошадей под капотом машины, стоящей в гараже, который, в свою очередь, заменил прежде необходимый сарай» [8. С. 87]. Однако другим исследователям такая аналогия не кажется корректной: «Возможности, которые предоставляет Интернет, делают его не просто инструментом. Это основополагающая система, которая, скорее, служит дорогой для наших путешествий, чем лошадью, на которой мы едем» [9]. В этом контексте право на доступ к Интернету можно уподобить как свободе передвижения (первое поколение), так и обязательствам государства создавать и поддерживать соответствующую инфраструктуру (второе поколение).

Подводя итог, можно сказать, что право на доступ к Интернету в самом общем виде может быть определено как право беспрепятственного подключения к Интернету и осуществления в нем различных видов деятельности. Оно охватывает притязания, которые по своей юридической природе относятся как к первому, так и ко второму поколению прав человека. Притязания в рамках прав первого поколения сводятся к свободе от какого бы то ни было вмешательства со стороны как государства, так и частных лиц в отношении доступа к сети Интернет в целом и любым интернет-ресурсам и их использования (получения и распространения информации, установления и поддержания коммуникации и т. п.).

Данные притязания могут рассматриваться как одно из новых проявлений индивидуальной свободы – свободы доступа в виртуальную среду (цифровое пространство) и функционирования в ней. При этом, как уже отмечалось, свобода функционирования в интернет-пространстве не является новым самостоятельным правом человека, а представляет собой реализацию традиционных прав в новых (виртуальных, цифровых) условиях. С юридической точки зрения регулирование их обеспечения и защиты не содержит в себе ничего нового, за исключением («всего лишь») необходимости учитывать технологические ограничения, налагаемые цифровой средой.

В качестве нового права может рассматриваться только право на сам доступ к Интернету. Как право первого поколения оно предполагает негативные обязательства государства не запрещать и не ограничивать доступ к Интернету (отдельным интернет-ресурсам) и его позитивные обязательства по установлению правового регулирования доступа к Интенету, в том числе его допустимых ограничений, и предоставлению защиты от неправомерных ограничений, в том числе и со стороны частных лиц.

Список литературы

1. Саликов М. С., Несмеянова С. Э. Права и свободы человека в сети интернет: особенности реализации и защиты // Российское право: образование, практика, наука. 2019. № 1.

2. Организация Объединенных Наций. Генеральная Ассамблея. URL: https://undocs.org/pdf?symbol=ru/A/HRC/17/27

3. Совет по правам человека. Резолюция 7/36 от 28 марта 2008 г. Мандат Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение // Организация Объединенных Наций. Совет по правам человека. URL: http://ap.ohchr.org/documents/R/HRC/resolutions/A_HRC_RES_7_36.pdf

4. Всеобщая декларация прав человека. Принята резолюцией 217 A (III) Генеральной Ассамблеи ООН от 10 декабря 1948 г. // Организация Объединенных Наций. URL: https://www.un.org/ru/documents/decl_conv/declarations/declhr.shtml

5. Талапина Э. В. Права человека в Интернете: Публично-правовой аспект. М.: Проспект, 2020.

6. Tomalty J. Is There a Human Right to Internet Access? // Philosophy Now. 2017. Vol. 118.

7. Варламова Н. В. Цифровые права – новое поколение прав человека? // Труды института государства и права Российской академии наук. 2019. Т. 14, № 4.

8. Cerf V. G. Emergent Properties, Human Rights, and the Internet // IEEE Internet Computing. 2012. Vol. 16. Iss. 2.

9. Sniadecki T. D. A Road Compared to a Horse: An Examination of Internet Access as a Human Right // Grand Valley State University. Honors Projects. 2014. URL: http:// scholarworks.gvsu.edu/honorsprojects/283

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ЧАСТНО-ПРАВОВЫХ (ЦИВИЛИСТИЧЕСКИХ) ОТНОШЕНИЙ

DIGITAL TECHNOLOGIES IN THE SYSTEM OF PRIVATE-LEGAL (CIVILISTIC) RELATIONS

Е. Н. Абрамова,
кандидат юридических наук, доцент,
Санкт-Петербургский государственный экономический университет

ВОЛЕИЗЪЯВЛЕНИЕ НА ЗАКЛЮЧЕНИЕ СДЕЛКИ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Аннотация. В статье ставится вопрос о правовой природе волеизъявления в информационной системе и его месте в системе традиционных способов волеизъявления. Делается вывод о квалификации волеизъявления в информационной системе в качестве прямого способа изъявления воли и способа заключения сделки в письменной форме. На основе сделанных выводов даются рекомендации по совершенствованию действующего законодательства путем ликвидации существующих пробелов в квалификации заключения сделки в информационной системе в качестве дополнительного требования к простой письменной форме сделки, установления общих правил его правового режима и установления последствий его несоблюдения.

Ключевые слова: сделка, заключение сделки, информационная система, дополнительное требование к простой письменной форме сделки, способ волеизъявления, договор присоединения, цифровой способ заключения договора

AGREEMENT IN INFORMATION SYSTEM

Abstract. The article raises the question of the legal nature of expression of will in the information system and its place in the system of traditional methods of expression of will. A conclusion is made about the qualification of the expression of will in the information system as a direct method of expressing the will and a method of concluding a transaction in writing. Based on the conclusions made, the author makes recommendations for improving the current legislation by eliminating existing gaps in the qualification of concluding a transaction in the information system as an additional requirement for a simple written form of the transaction, establishing general rules of its legal regime and establishing the consequences of its non-compliance.

Keywords: transaction, conclusion of a transaction, information system, additional requirement for a simple written form of a transaction, method of expression of will, agreement of adhesion, digital method of concluding an agreement

Технический прогресс в информационно-коммуникационной сфере породил множество новых тенденций и проблем цивилистики. В частности, в литературе отмечается процесс «полной виртуализации», или «дематериализации договорных отношений» [1. P. 233]. В связи с развитием цифровой экономики традиционное волеизъявление на заключение сделки пополнилось новой разновидностью – выражением воли в информационной системе. Поэтому возникает вопрос о правовой природе волеизъявления в информационной системе и его месте в системе традиционных способов изъявления воли.

В отличие от традиционных видов прямого волеизъявления – устного и письменного, выражение воли в информационной системе осуществляется без использования словесной речи, путем нажатия или выбора определенной опции на экране. Поскольку для прямого волеизъявления характерно выражение воли путем прямой передачи его содержания с помощью слов, неоднозначным является отнесение волеизъявления в информационной системе к прямому способу волеизъявления. Волеизъявление в информационной системе фактически не является ни устным, ни письменным, поскольку ни устная, ни письменная речь субъектом при этом не используется. Он выражает свою волю «молча», с помощью действий. Таким образом, возникает вопрос о том, каким способом волеизъявления является изъявление воли в информационной системе: прямым, косвенным, посредством молчания или новым для цивилистики способом волеизъявления.

Очевидным представляется вывод о том, что «технократическое» волеизъявление, как условно можно его обозначить, не является изъявлением воли посредством молчания, поскольку для последнего характерно отсутствие активного поведения субъекта в целях выражения своей внутренней воли. Молчание само по себе не демонстрирует волю субъекта и качественно отражает нейтральную реакцию, отсутствие воли и ее изъявления. Лишь благодаря прямому указанию закона молчание хотя и не является, но считается выражением определенной, указанной в этом законе воли. «Технократическое» волеизъявление, в отличие от молчания, не является нейтральной реакцией и качественно демонстрирует совершенно определенную позицию субъекта, оно по своей сути является активным выражением совершенно определенной воли.

Фактически этот способ более близок косвенному волеизъявлению, когда воля выражается путем конклюдентных действий, поскольку при этом внутренняя воля выражается не непосредственно, путем передачи ее содержания, а путем совершения действия. Однако квалифицировать такой способ волеизъявления в качестве конклюдентного действия не представляется целесообразным.

С одной стороны, такого действия недостаточно для признания его несомненным свидетельством намерения заключить сделку, а с другой стороны, оно является более чем свидетельством намерения, оно однозначно порождает гражданско-правовые последствия. Таким образом, «технократическое» волеизъявление одновременно и больше, чем конклюдентное действие, и меньше, чем оно. Рассмотрим два данных, противоречащих друг другу, признака волеизъявления в информационной системе подробнее.

С одной стороны, нажатие клавиши пальцем, голосом или с помощью другого физического воздействия на техническое средство не «позволяет с несомненностью прийти к заключению о намерении совершить сделку», а именно такой признак конклюдентного волеизъявления является классическим и аксиоматичным [2. С. 254]. Сомнения в наличии внутренней воли на заключение сделки, заключаемой в информационной системе, не могут отсутствовать по причине самой природы информационной системы как среде общения контрагентов. Последние коммуницируют дистанционно, они не видят друг друга и элементарно не знают, точно ли «на другой стороне экрана» тот субъект, от имени которого выражается воля. Совпадение ожидаемого и фактического контрагента лишь презюмируется, но может быть и опровергнуто. Действие по нажатию клавиши может быть произведено не только в результате преступных или иных неправомерных деяний, но и по ошибке, в результате технического сбоя, непредвиденных жизненных ситуаций. При этом в заблуждение относительно воли контрагента может быть введена любая сторона сделки, как изъявившая или якобы изъявившая свою волю в информационной системе, так и получившая «отсутствующее» согласие на сделку. Тем не менее, как и в случае молчания, «технократическое» волеизъявление презумируется по закону надлежащим и состоявшимся. При этом не разработаны механизмы опровержения данной презумпции, что явно нарушает права участников гражданского оборота на защиту своих нарушенных прав, поскольку ставит их в состояние правовой неопределенности и беззащитности. Возможно при этом, что такие способы не могут быть безупречными по объективным техническим причинам.

С другой стороны, несмотря на неочевидность наличия внутренней воли, «технократическое» волеизъявление активизирует работу программного алгоритма и влечет совершенно определенные правовые последствия, иногда связанные не только с фактом заключения сделки, но и с фактом ее исполнения и обеспечения исполнения (как, например, в случае смарт-контракта). Таким образом, в отличие от конклюдентного способа заключения сделки, который требует анализа действий субъекта, в случае «технократического» волеизъявления нажатие на клавишу или иное физическое воздействие на техническое средство не анализируется в условиях обстановки совершения, а сразу не только считается выражением согласия, но и активизирует правовые результаты такового.

Таким образом, хотя «технократическое» волеизъявление и является фактически физическим воздействием на техническое средство, т. е. действием, а не выражением словесного содержания, его следует относить именно к прямому, а не косвенному способу выражения воли. Такое действие по нажатию выбранной опции на экране с правовой точки зрения является не выражением содержания воли, а выражением согласия на то содержание, с которым субъект ознакомился на информационной системе и к которым желает присоединиться.

Следовательно, «технократическое» волеизъявление является аналогом собственноручной и рукописной подписи, т. е. способом заключения сделки. А способ волеизъявления при этом – прямой письменный, поскольку электронный документ приравнен действующим законодательством к письменной форме сделки. Подписание традиционного письменного документа возможно двумя разными

способами: путем составления единого документа или путем обмена документами. При этом обмен документами всегда производится с помощью создания содержания сделки самим субъектом, а составление единого документа возможно в двух вариантах – когда содержание сделки формируется двумя сторонами совместно либо когда содержание сделки формируется только одной стороной, а другие субъекты лишь присоединяются к выработанным первой стороной условиям. Сделка в информационной системе порождает лишь один из указанных вариантов, которые предлагаются традиционными способами выражения воли и заключения сделки. Содержание сделки, заключаемой в информационной системе, всегда формируется только одной ее стороной, а вторая может лишь либо присоединиться к нему, нажав соответствующую клавишу или выполнив иное оговоренное в информационной системе действие, либо отказаться от заключения сделки.

Таким образом, сделка, заключенная в информационной системе, всегда является договором присоединения. Поэтому независимо от упоминания об этом в законодательстве, к ней должны применяться нормы гражданского законодательства о защите слабой стороны договора и о договоре присоединения.

Требование о заключении сделки в информационной системе следует считать дополнительным требованием к простой письменной форме сделки. При этом существуют сделки, которые могут быть заключены исключительно в информационной системе. При этом последствия несоблюдения такого дополнительного требования к форме сделки могут быть предусмотрены в законе, установившем обязательность заключения сделки в информационной системе [5]. Следует учитывать, что согласно действующему правилу ст. 444 ГК РФ, если последствия несоблюдения дополнительного требования к простой письменной форме сделки не предусмотрены законом, установившим его, применяются общие последствия несоблюдения простой письменной формы сделки, предусмотренные национальным законодательством, т. е. сделка остается действительной, но в случае спора сторонам запрещается ссылаться на показания свидетелей в доказательство факта и условий заключения сделки. Такое последствие явно противоречит нормам тех нормативных актов, которые сегодня предусматривают обязательность данного дополнительного требования (например, сделки с цифровым финансовым активом [4], цифровым утилитарным правом [3] и др.). Поэтому такие акты требуют внесения в них дополнений в части указания в качестве последствия заключения сделок с цифровыми правами вне информационной системы – например, недействительности сделки.

Список литературы

1. Dernozot A. Chroniques. 1-er ocobre – 31 decembre 2017 // RTDCiv. Revue trimestrielle de droit civil. Janvier-mars, 2018.

2. Иоффе О. С. Советское гражданское право. М.: Юридическая литература, 1967.

3. О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 2 августа 2019 № 259 // СПС «КонсультантПлюс».

4. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 31 июля 2020 № 259 // СПС «КонсультантПлюс».

5. Казанцев Д. А. Проблемы и перспективы регулирования отношений в рамках сделки, совершенной с участием искусственного интеллекта // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 438-463. EDN JYQAZW

Е. Н. Агибалова,
кандидат юридических наук, доцент,
Волгоградский институт управления –
филиал Российской академии народного хозяйства
и государственной службы при Президенте Российской Федерации
А. А. Рыжова,
стажер,
Нотариальная палата Волгоградской области

ДЕЛИКТНАЯ ОТВЕТСТВЕННОСТЬ НОТАРИУСА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ НОТАРИАТА

Аннотация. В статье представлено описание законодательной конструкции деликтной ответственности нотариуса за совершение правонарушения в своей деятельности. Анализируется состав такого гражданского правонарушения и применение этого состава в контексте функционирования нотариата на практике. Отмечается, что в условиях функционирования единой информационной системы нотариата необходимо дополнить конструкцию деликтной ответственности нотариуса ответственностью администратора информационной системы.

Ключевые слова: нотариат, ответственность нотариуса, единая информационная система нотариата, цифровизация нотариата, деликтная ответственность

TORT LIABILITY OF A NOTARY IN THE CONDITIONS OF DIGITALIZATION OF A NOTARY

Abstract. The article describes the legislative structure of the tort liability of a notary for committing an offence in their activity. Authors analyze the composition of such a civil offense and the application of this composition in the context of the functioning of the notary's unified information system (UIS) in practice. Authors conclude that in the conditions of the functioning of the notary's UIS, it is necessary to supplement the construction of the notary's tort liability with the responsibility of the information system administrator.

Keywords: notary, notary's responsibility, notary's unified information system, notary digitalization, tort liability

Исследование юридических практик в аспекте темы цифровизации права предполагает, что ученый должен иметь в виду две детали. Во-первых, он дол-

жен составить представление о содержании исследуемой юридической практики вне контекста цифровизации. Иными словами, в нашем случае первичной задачей для нас является определение параметров практики привлечения нотариусов к деликтной ответственности за их действия: состав правонарушения, применяемые нормы, сложившаяся практика и особенности применения норм. Во-вторых, исследователь должен на основании этого представления о существующих юридических практиках определить, как именно цифровизация влияет на содержание этих практик, как может меняться правовая квалификация отношений, в которые внедряется элемент цифровизации. По вышеуказанным соображениям мы начнем с общего анализа правового регулирования и практики ответственности нотариуса за совершаемые им действия.

Основная норма в российском законодательстве, регулирующая привлечение нотариуса к ответственности, это статья 17 Основ законодательства Российской Федерации о нотариате, утвержденных Постановлением Верховного Совета РФ от 11.02.1993 № 4462-1 [6]. Абзац первый статьи 17 устанавливает полную имущественную ответственность нотариуса за вред, причиненный по его вине имуществу физического или юридического лица по причине совершения незаконного действия.

Мы можем наблюдать по тексту, что абзац первый статьи 17 Основ устанавливает приблизительный состав правонарушения, порождающего возникновение обязательства возместить причиненный вред. В отношении состава гражданского правонарушения в целом существует достаточно много разночтений. И в рамках настоящей статьи мы будем понимать состав гражданского правонарушения с ориентиром на практику – как совокупность обстоятельств, необходимых и достаточных для возникновения обязательства по возмещению вреда [7. С. 22].

Объектом (предметом) правонарушения закон определяет имущество граждан и юридических лиц. Это означает, что статья 17 Основ ограничивает нотариуса ответственностью только за имущество граждан, а причинение вреда жизни и здоровью не охватывается нормами Основ. Объективной стороной рассматриваемого правонарушения является совершение нотариусом незаконного действия, ставшего причиной ущерба для имущества физического или юридического лица. Субъективная сторона проявляется в форме вины нотариуса за совершенное действие. Субъектом же данного правонарушения является частнопрактикующий нотариус, его работники и замещающее его лицо. Ответственность нотариуса, работающего в государственной нотариальной конторе, устанавливается в абзаце 7 цитируемой статьи 17 Основ. Она предопределяется тем, что за действия такого нотариуса отвечает государство. Однако рассмотрение специфики ответственности нотариусов, работающих в государственной конторе, не является предметом рассмотрения в настоящей статье по причине небольшой распространенности данной формы нотариальной практики.

Абзацы 2 и 3 статьи 17 Основ дополняют этот состав правонарушения, указывая на дополнительные детали объективной стороны. В частности, ответственность частнопрактикующего нотариуса также наступает за неправомерный отказ в совершении нотариального действия и за разглашение данных о совершении нотариального действия.

Вместе с тем описанная конструкция состава правонарушения довольно редко применяется на практике. Это объясняется, во-первых, личной заинтересованностью частнопрактикующих нотариусов в качестве выполняемой работы, а во-вторых, трудностью доказывания причинной связи между действиями нотариуса и вредом имуществу. Эта сложность состоит в том, что зона возможных манипуляций с имуществом существенно ограничена, за исключением некоторых действий по типу охраны наследственного имущества [8. С. 126-127]. Поэтому и причинная связь между действиями нотариуса и причинением вреда достаточно труднодоказуема.

Как правило, незаконные действия нотариусов сами по себе не влекут негативных последствий, поскольку нотариусы не являются непосредственными участниками гражданского оборота, а их функция заключается в обеспечении действий непосредственных участников гражданского оборота. Понимание обеспечительного характера нотариальной функции позволяет сделать вывод об особенности деликтной ответственности нотариуса в целом и ее проблематике. Совершение нотариусом незаконного действия является лишь предпосылкой причинения вреда от действий или бездействия участника гражданского оборота.

Из последнего соображения вытекает закономерный вопрос: в каком размере следует оценивать причиненный нотариусами вред, если, строго говоря, их действия непосредственно не приводят к причинению вреда? Эту проблему, возникающую и на практике, можно обозначить как трудность определения содержания понятия вреда, причиненного нотариусом [1].

Даже анализ учебной литературы об ответственности нотариуса не позволяет оттенить проблематику данной юридической конструкции [3. С. 110-113]. Кроме того, еще одной проблемой становится неоднозначная квалификация статьи 17 Основ в контексте главы 59 Гражданского кодекса Российской Федерации, которая устанавливает общие положения об обязательствах из причинения вреда. С одной стороны, налицо сходство анализируемых составов и природы ответственности. С другой стороны, при наличии специальной нормы (статьи 17 Основ) общие нормы должны применяться лишь субсидиарно на случаи, когда соответствующие отношения не были урегулированы. Вместе с тем даже в практике высших судов мы встречаемся с делами, в которых рассматриваются случаи ответственности нотариуса. Обратимся к ним для понимания, как обозначенная нами проблематика раскрывается на практике.

Так, в Обзоре судебной практики Верховного Суда Российской Федерации № 1 за 2021 год, утвержденном Президиумом Верховного Суда РФ 07.04.2021 [4], описываются обстоятельства дела, согласно которым нотариус не удостоверился должным образом в личности поверенного, действовавшего по поддельному паспорту, в результате чего квартира доверителя была продана. Сделка была признана недействительной, регистрационные действия отменены, доверенность признана также недействительной. Суд первой инстанции исходил из описанной нами логики обеспечительного характера функций нотариуса и указал, что вред причинен не нотариусом, а ненадлежащим представителем. Однако апелляционная инстанция и Верховный Суд установили, что неправомерные действия представителя не отменяют обязанности нотариуса удостоверить личность при совершении нотари-

альных действий, установленной ст. 42 Основ. Поэтому за неисполнение обязанности следует ответственность. Однако основной вопрос, который мы поднимали выше, о размере ответственности нотариуса остался в Обзоре без внимания.

Полагаем, что цифровизация нотариата хотя и значительно упростила процессы делопроизводства нотариусов, а также сделала более доступным получение услуг нотариусов, в вопросе ответственности выступила фактором, который усугубляет названную проблему. Поясним сказанное.

Введенная в законодательство о нотариате в 2013 году единая информационная система нотариата, закрепленная в главе VII.1 Основ, стала основой правового регулирования цифровизации нотариата, а программное обеспечение «еНот» – ее содержательным наполнением. Как отмечают разработчики программного обеспечения, у ЕИС нотариата есть два интерфейса: веб-интерфейс и программный интерфейс. Веб-интерфейс нужен для просмотра баз данных информационных блоков и работы с подсистемами ЕИС с помощью обычного браузера. Программный интерфейс сервера ЕИС предназначен для организации взаимодействия со специальным приложением «еНот», реализующим прикладные функции системы на рабочем месте пользователя ЕИС. Каждый из пользователей ЕИС имеет свою собственную локальную базу данных, содержащую частичную репликацию содержимого базы данных сервера ЕИС, а также свою собственную информацию, частично реплицируемую в базу данных сервера ЕИС. Обмен информацией между пользователями системы и сервером ЕИС выполняется с помощью приложения «еНот» [2].

Подробная остановка на указанных деталях не случайна. Дело в том, что в обычных условиях гражданского оборота нотариус является лишь промежуточной инстанцией между его участниками, как в примере со сторонами договора. Он в этих отношениях не участвует, но влияет на них косвенно через нотариальные действия. Внедрение информационных систем в деятельность нотариуса только усиливает эту ситуацию. Рассмотрим заявленный тезис на примере.

Статья 53.1 Основ устанавливает возможность удостоверения сделки двумя и более нотариусами, если в сделке участвуют два и более лица без их совместного присутствия. Это, с одной стороны, позволяет гражданам, находящимся в разных городах, удостоверить сделку без необходимости находиться на одной территории. С другой стороны, такая возможность свидетельствует о присутствии посредника в таких взаимоотношениях. А именно – системы и тех, кто ее обслуживает. Ведь нотариус взаимодействует с описанным выше веб-интерфейсом, предназначенным для взаимодействия с пользователем. Программный же интерфейс недоступен для нотариуса, если он не является еще и программистом. Однако веб-интерфейс является той основой, за счет которой функционируют система в целом и приложение «еНот» у нотариусов. В связи с эти возникает вопрос: кто должен нести ответственност: в случае программной ошибки в организации такой сделки нотариусом?

Например, в абзаце 5 статьи 53.1 Основ описан порядок удостоверения сделки двумя и более нотариусами. Он также дополнен подзаконным актом – Порядком взаимодействия нотариусов с единой информационной системой нотариата при удостоверении сделки двумя и более нотариусами [5]. Порядок представлен в тексте закона как ряд сменяющих друг друга этапов взаимодействия нотариусов

с участниками сделки, между собой, а также с информационной системой, которые в целом образуют порядок совершения нотариального действия. Помимо классических действий нотариусов и сторон в процессе удостоверения сделки, представляется любопытным один абзац этого порядка, который выполняется не нотариусом, не стороной сделки, а самой системой. Это абзац 8 статьи 53.1 Основ, который изложен следующим образом: «неизменность текста сделки в электронной форме обеспечивается средствами единой информационной системы нотариата». Таким образом, имеет место указание на то, что неизменность текста сделки, то есть действие, которое должно было бы обеспечиваться в обычных условиях нотариусом, обеспечивается информационной системой. В связи с этим вопрос, заданный нами ранее, еще более актуализируется. Если в законе прямо указано, что неизменность текста сделки обеспечивается системой, то будет ли нести ответственность за нарушение этой неизменности нотариус в случае технической ошибки?

Поскольку ЕИС нотариата не является полностью автономной системой и в буквальном смысле не может самостоятельно ничего обеспечивать, а требует воздействия извне, для корректного распределения ответственности необходимо скорректировать состав ответственности за нарушения в сфере производства нотариальных действий. Полагаем, для этого необходимо введение субъекта ответственности – администратора информационной системы и включение в текст закона перечня действий, которые недопустимы при взаимодействии с системой, так как могут нарушить права лиц, обратившихся к нотариусу.

Статья 17 Основ, которая была детально нами разобрана выше, также не была адаптирована в связи с введением положений о ЕИС нотариата. Несмотря на это, дистанционно удостоверенные сделки содержат в себе те же риски, что и сделки, удостоверенные в классической форме. А потому и те и другие должны предусматривать равную ответственность за незаконные действия, повлекшие ущерб имуществу гражданина, и за разглашение данных.

И в отношении разглашения данных также в связи с цифровизацией появляются риски так называемых сливов данных, организованных заинтересованными лицами. Представляется, что в данном случае было бы необоснованным привлекать к ответственности нотариусов. Во избежание подобных случаев необходимо установление оговорок в законодательстве о нотариате, которые предусматривали бы нового субъекта ответственности – администратора информационной системы.

Список литературы

1. Акимочкин Д. Несет ли нотариус ответственность перед сторонами удостоверенной им сделки в случае признания ее недействительной? URL: https://garant-vrn.ru/vopros-otvet/vo261211

2. Информация о программе «еНот». URL: https://www.triasoft.com

3. Нотариальное право: учебник / Б. М. Гонгало, Т. И. Зайцева, И. Г. Медведев и др.; под ред. В. В. Яркова. 2-е изд., испр. и доп. М.: Статут, 2017. 576 с.

4. Обзор судебной практики Верховного Суда Российской Федерации № 1 за 2021 год, утв. Президиумом Верховного Суда РФ 07.04.2021 // Бюллетень Верховного Суда РФ. 2021. № 7.

5. Об утверждении Порядка взаимодействия нотариусов с единой информационной системой нотариата при удостоверении сделки двумя и более нотариусами: приказ Минюста России от 30.09.2020 № 222 // СПС «КонсультантПлюс»

6. Основы законодательства Российской Федерации о нотариате, утв. ВС РФ 11.02.1993 № 4462-1 // Российская газета. 1993. № 49.

7. Тычинин С. В., Туршук Л. Д. Состав гражданского правонарушения как основание деликтной ответственности // Современное общество и право. 2019. № 3(40). С. 22-28.

8. Харитонова Ю. С. Ответственность сторон по договору доверительного управления наследственным имуществом предпринимателя // Lex russica. 2017. № 5. С. 126-135.

Н. Г. Вилкова,
заслуженный юрист Российской Федерации,
доктор юридических наук, профессор,
Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ИСПОЛНЕНИЕ МЕЖДУНАРОДНОГО КОНТРАКТА

Аннотация. В статье анализируется деятельность Международной торговой палаты по разработке и предложению бизнесу типовых контрактов, оформляющих различные виды коммерческих транзакций: международная купля-продажа, строительный подряд, дистрибуция, соглашения о консорциуме и стартапы. Наличие типового контракта, созданного с применением опыта практиков из различных стран и юрисдикций, значительно облегчает разработку и согласования содержания конкретной сделки ее участниками, экономит время и позволяет найти наиболее выгодные для сторон условия. В статье рассматриваются Единообразные правила МТП для цифровых торговых транзакций (Uniform Rules for Digital Trade Transactions), который совместно с Типовым контрактом МТП международной купли-продажи представляет первый практический опыт безбумажной сделки (Digital Trade Transaction (DTT)).

Ключевые слова: типовые контракты Международной торговой палаты, цифровизация торговых транзакций, цифровизация практик торгового финансирования, система обработки данных, электронная запись, электронная подпись, функции, осуществляемые участниками транзакции

DIGITAL TECHNOLOGIES AND PERFORMANCE OF AN INTERNATIONAL CONTRACT

Abstract. The article analyzes the activities of the International Chamber of Commerce in developing and offering to business different types of commercial transactions: international sale of goods, construction contracts, distribution, consortium agree-

ment and start-ups. Model contract created on the basis of the experience of practitioners from various countries and jurisdictions, help parties to develop terms and conditions of a particular transaction, saves time and allow to find the most favorable conditions. The article discusses the ICC Uniform Rules for Digital Trade Transactions, which, together with the ICC Model Contract for International Sale and Purchase, represents the first practical experience of a paperless transaction (Digital Trade Transaction (DTT)).

Keywords: model contracts of the International Chamber of Commerce, digitalization of trade transactions, digitalization of trade finance practices, data processing system, electronic record, electronic signature, functions performed by participants and transactions

Настоящая публикация является продолжением опубликованной в Сборнике I Международной конференции «Цифровые технологии и право» статьи «Цифровые технологии и международный арбитраж» [1], в которой указывалось на Инструментарий стандартов для трансграничной безбумажной торговли, разработанный ICC и Всемирной торговой организацией (WTO) в 2022 г.

В статье рассмотрим новую разработку Международной торговой палаты – Унифицированными правилами ICC для цифровых торговых транзакций.

Международная торговая палата (ICC) является институциональным представителем более 45 миллионов компаний в более чем 100 странах, значительный вклад в результативность деятельности ICC оказывают более 90 национальных комитетов, действующих на всех континентах. В нашей стране Национальный комитет ICC Russia был создан в 2000 г., ознакомиться с его деятельностью можно по ссылке https://iccwbo.ru/

Основной задачей ICC является продвижение международной торговли, что реализуется через комиссии ICC, прежде всего через Банковскую комиссию и Комиссию по коммерческому праву и практике, членом которой является автор данной публикации.

Банковской комиссией были разработаны следующие документы, получившие широкое распространение в практике банков по всему миру: Международная стандартная практика гарантии по требованию для URDG 758, редакция 2010. ICC Pub. No. 814E, Унифицированные правила для гарантий по требованию с типовыми формами (URDG), ICC Pub. No. 814E, Унифицированные правила и обычаи для документарных аккредитивов ICC Pub. No. 600, Унифицированные правила по инкассо, ICC Pub. No 522, Международная стандартная банковская практика проверки документов соответствии с UCP 600, ICC Pub. No 745E, Унифицированные правила для банковских платежных обязательств ICC Pub. No P750E).

Для продвижения цифровизации практик торгового финансирования Банковская комиссия ICC выпустила электронные правила в виде электронных дополнений к существующим Унифицированным правилам инкассо (URC 522) и Унифицированным правилам и обычаям для документарных аккредитивов (UCP 600). eURC и eUCP устанавливают правила для электронных записей, связанных с существующими, хорошо зарекомендовавшими себя продуктами торгового финансирования. Эти электронные правила являются дополнением к UCP и URC

и предназначены для представления электронных документов в соответствии с аккредитивами и инструкциями по инкассо соответственно. Поэтому они продолжают действовать самостоятельно наряду с URDTT.

Следующим этапом деятельности Банковской комиссии ICC явились разработка и принятие в 2021 г. Унифицированных правил ICC для Цифровых торговых транзакций (Uniform Rules for Digital Trade Transactions), публикация ICC No. KS102E, вступили в силу с 1 октября 2021 г.) и Руководство по использованию этих Правил (Implementing Uniform Rules for Digital Trade Transactions, URDTT, version 1, публикация ICC No KS103E, принято в 2022 г.).

Цифровая торговая сделка (DTT) – это представление базовой транзакции, процесс, посредством которого условия коммерческого контракта между продавцом и покупателем фиксируются и выполняются. По своей сути DTT отличается от коммерческого контракта. Существует возможность указать два набора электронных записей в условиях DTT: i) Электронные записи, подтверждающие факт продажи и покупки товаров или услуг; ii) Электронные записи, подтверждающие фактическую доставку/получение этих товаров или услуг.

Во Введении к Унифицированным правилам указывается: чтобы оценить истинную ценность URDTT, нужно выйти за рамки традиционных инструментов; думать за пределами традиционного нормотворчества; думать за пределами существующих способов делать бизнес. URDTT – это не просто набор правил для банков; правила распространяются на корпоративный мир, а также на растущее сообщество небанковских поставщиков услуг. URDTT предназначены для управления цифровым ландшафтом с учетом последних событий, а не только в технологии распределенного реестра, но и в использовании искусственного интеллекта, естественной обработки языка, машинном обучении, анализе данных, смарт-контрактов, смарт-объектов и интернета вещей, все из которых окажут существенное влияние на то, как мы будем осуществлять бизнес в будущем.

Унифицированные правила ICC для цифровых торговых транзакций возникли как продолжение Унифицированных правил банковских платежных обязательств (далее – URBPO). Первоначальный план Банковской комиссии состоял в совершенствовании URBPO, однако в последующем было решено создать самостоятельный документ – Унифицированные правила ICC для цифровых торговых транзакций (далее: URDTT). Таким образом, в настоящее время действуют оба документа – URBPO и URDTT.

Унифицированные правила ICC для цифровых торговых транзакций (URDTT) предназначены: (a) для полной цифровой среды; (b) они должны быть нейтральными в отношении технологий и стандартов обмена сообщениями; и (c) распространяться на все корпоративное пространство, включая коммерческие сделки и растущее сообщество небанковских поставщиков финансовых услуг. Они имеют целью совместимость с документами ЮНСИТРАЛ: Типовым законом ЮНСИТРАЛ об электронной торговле 1996 г. [2], Типовым законом ЮНСИТРАЛ об электронных подписях 2001 г. [3], Конвенцией ООН об использовании электронных сообщений в международных договорах 2005 г. [4], Типовым законом ЮНСИТРАЛ об электронных передаваемых записях 2017 г. [5].

В Руководстве по использованию URDTT указывается, что выполнение условий DTT не является синонимом исполнения коммерческого контракта. Условия DTT выполняются путем подачи электронных записей, указанных в DTT, а коммерческий контракт реализуется путем его исполнения (сторонами). Платежное обязательство (PO) всегда независимо от коммерческого контракта и становится независимым от DTT после выполнения условий последнего. Поскольку Платежное обязательство FSP добавляется к PO и неотделимо от него, то же самое относится и к Платежному обязательству FSP.

Вместе с тем в разделе Руководства «Соглашение покупателя/продавца» указывается, что базовый коммерческий контракт должен быть подробно описан, и обращается внимание на то, что Типовой контракт международной купли-продажи ICC представляет собой шаблон для представления набора четких и кратких стандартных договорных условий для наиболее часто встречающегося в международной практике договора. Этот типовой договор специально адаптирован для сделок, регулируемых Конвенцией ООН о международной купле-продаже товаров (CISG), которая применяется ко все более крупным объемам международных продаж. Целью CISG является обеспечение современного, единообразного и справедливого режима для договоров международной купли-продажи товаров.

Моделью для составления контракта является Типовой контракт ICC международной купли-продажи (готовые изделия), в котором отражены четкие и краткие стандартные договорные условия для наиболее распространенной международной сделки. Этот типовой договор специально адаптирован для сделок, регулируемых Конвенцией ООН о международной купле-продаже товаров (CISG), которая применяется к все более крупным объемам международных продаж. Целью CISG является обеспечение современного, единообразного и справедливого режима для договоров международной купли-продажи товаров.

Унифицированные правила ICC для цифровых торговых транзакций (URDTT) включают 17 статей, в которых предлагается регулирование вопросов цифровизации и таких правовых вопросов, как определения, толкование, передача прав, форс-мажор и применимое право. Таким образом стороны сделки международной купли-продажи и оказания услуг получили возможность действовать в цифровой среде.

Структура Правил представляет собой одну из основных транзакций по купле-продаже и предоставлению услуг, которые Основные стороны согласились подтвердить в электронном виде, включая способ оплаты, который сам по себе является электронным.

В ст. 1 приводятся определения, которые имеют значение для четкого понимания субъектов транзакции и реализуемых в сделке процессов. Среди участников транзакции выделяются Продавец (продавец товаров или услуг), Покупатель (приобретатель товаров или услуг), Поставщик финансовых услуг (FSP, финансовое учреждение или Лицо, кроме Основной стороны), Основная сторона (Покупатель или Продавец), Сторона (Основная сторона или Поставщик финансовых услуг), Платежное обязательство FSP (безотзывное обязательство провайдера финансовых услуг по осуществлению платежа по предъявлении или в фиксированную или определяемую в будущем дату Бенефициару платежного обязательства).

Далее даются следующие определения. Система обработки данных означает компьютеризированную, электронную или любые иные автоматизированные средства, используемые для обработки и манипулирования данными, инициирования действия или ответа на данные сообщения полностью или частично.

Электронная запись означает данные, созданные, сгенерированные, отправленные, переданные, полученные или сохраненные электронными средствами, включая при необходимости всю информацию, логически связанную тем или иным образом вместе, чтобы стать частью записи, независимо от того, сгенерирована ли она одновременно или нет, то есть:

– возможность аутентификации в отношении очевидной личности Подателя и очевидный источник данных, содержащихся в нем, и относительно того, остались ли они полными и неизменными;

– возможность проверки на соответствие условиям Цифровой торговой сделки.

Электронная подпись означает или логический процесс обработки данных, приложенный к/или логически связанный с Электронной записью, выполненной или принятой Стороной или Лицом для идентификации этой Стороны или Лица и для аутентификации Электронной записи этой Стороной или Лицом.

В ст. 4 и 5 URDTT перечислены функции, осуществляемые участниками транзакции. Роль Продавца включает:

I. поставку товаров или оказание услуг в соответствии с условиями и положениями Цифровой торговой сделки.

II. предоставление информации, необходимой для обеспечения поставки товаров или предоставления услуг.

III. предоставление любой дополнительной информации, которая может потребоваться, включая Электронные записи сертификатов об инспекции (осмотре) и о страховании. Роль Покупателя включает:

I. получение товаров или услуг, которые соответствуют условиям и положениям Цифровой торговой транзакции.

II. при соблюдении условий Цифровой торговой транзакции Продавцом, взявшим на себя Безусловное Платежное обязательство FSP, осуществляется платеж в соответствии с этим Платежным обязательством.

Роль Поставщика финансовых услуг включает:

i. Предоставление финансирования или снижение рисков Бенефициару или Покупателю или другому Поставщику финансовых услуг; или

ii. Осуществление платежа Бенефициару; или

iii. По просьбе Основной стороны или любого другого Бенефициара, в случае ее принятия, добавление своего Платежного обязательства FSP к Платежному обязательству и осуществление платежа по настоящему документу по предъявлении или в фиксированную или определяемую в будущем дату, в соответствии с условиями и положениям Платежного обязательства FSP.

Особо выделяется в ст. 5, что Поставщик финансовых услуг не имеет дело с товарами или услугами, к которым Электронная запись, представленная в рамках Цифровой торговой транзакции, может относиться. За исключением пред-

ставления им Электронной записи, Поставщик финансовых услуг не несет ответственности за форму, полноту, точность, подлинность, фальсификацию или юридическую силу любой Электронной записи или за общие или частные условия, указанные в Электронной записи; и не берет на себя никакой ответственности или обязательств за описание, количество, вес, качество, состояние, упаковку, доставку, стоимость или наличие товаров, услуг или других, исполнение, представленное в любой Электронной записи, или за добросовестность или действия или бездействие, платежеспособность, работу или репутацию грузоотправителя, перевозчика, экспедитора, грузополучателя или страховщика товаров или любого другого лица.

Важное значение имеют правила ст. 7 об электронных записях, поскольку в них фиксируются основные параметры транзакции:

a. Цифровая торговая транзакция должна указывать условия и положения, по которым будет определяться соответствие Электронной записи.

b. Все данные, относящиеся к Цифровой торговой транзакции, должны быть с ней связаны и отправлены Подателем Адресату в форме Электронной записи.

c. В одной Электронной записи может быть изложено любое требование о представлении одного или нескольких оригиналов или копий Электронной записи.

d. Электронная запись, представленная, но не требуемая условиями Цифровой торговой транзакции, может быть проигнорирована и ликвидирована Адресатом любым способом, который он считает уместным, и без какой-либо ответственности.

e. Если применимое право не требует иного, требование о том, чтобы информация была в письменной форме, это требование считается выполненным, когда Электронная запись, содержащая такую информацию, доступна Адресату и не подверглась повреждению данных.

f. Любое требование о представлении одного или нескольких оригиналов или копий Электронной записи удовлетворяется подачей одной Электронной записи.

g. Если применимое законодательство требует или разрешает доставку, передачу или владение Электронной записью, это требование или разрешение удовлетворяется передачей этой Электронной записи в исключительное распоряжение (под исключительный контроль) Адресата.

Поскольку не только акты коммерческой транзакции, но и оплата товара/услуг осуществляется в безбумажном виде, центральное значение имеют ст. 12 и 13 URDTT о реализации платежного обязательства.

Согласно ст. 12 Платежное обязательство возлагается на Покупателя при соблюдении Продавцом правил и условий Цифровой торговой транзакции. Когда Платежное обязательство считается условным, Покупатель обязан произвести оплату при соблюдении Продавцом условий Цифровой торговой транзакции. С этого момента Платежное обязательство автоматически изменяется и становится безусловным и независимым.

Также определяются те элементы, которые должны быть в Платежном обязательстве, в частности, указание на сделку, связывающую Платежное обязатель-

ство с Цифровой торговой транзакцией; наименование сторон, валюта и сумма платежа, условный или безусловный характер обязательства, применимое право.

В ст. 13 URDTT определен статут Платежного обязательства FSP, в частности, по запросу Основной стороны или иного Бенефициара Поставщик финансовых услуг может в любое время добавить свое Платежное обязательство FSP полностью или частично к Платежному. Важно, что Платежное обязательство FSP, добавленное к Платежному обязательству, является безусловным, отдельным и независимым от Цифровой торговой транзакции, даже если какая-либо ссылка на Цифровую торговую транзакцию включена в Платежное обязательство FSP. Покупатель несет ответственность в соответствии с Платежным обязательством, если иное не согласовано между каждой Основной стороной и любым другим Бенефициаром. Платежное обязательство FSP может быть изменено или аннулировано только при наличии соглашения каждой Основной стороны и любого другого Бенефициара. С этого момента Платежное обязательство FSP является измененным или аннулированным.

Существенное значение для стабильности цифровой транзакции имеют правила ст. 13 о внесении изменений в условия Цифровой торговой транзакции, согласно которым требуется согласие каждой Основной стороны, каждого Поставщика финансовых услуг, выпустившего Платежное обязательство FSP, и любого другого Бенефициара. С этого момента считается, что в Цифровую торговую транзакцию внесены изменения. Правила и условия Цифровой торговой транзакции, Платежного обязательства или Платежного обязательства FSP изменяются путем подачи новой Электронной записи, которая включает измененные критерии, Адресату существующей Электронной записи.

Для любой коммерческой транзакции, включая цифровую, важное значение имеют правила об освобождении от ответственности (форс-мажор). В ст. 16 URDTT определены параметры, за нарушение которых продавец (или другой Бенефициар) не несет ответственности: это последствия, возникающие в результате прерывания его деятельности, включая невозможность доступа к другой системе обработки данных, кроме его собственной, или сбой оборудования, программного обеспечения или сети связи. Основаниями освобождения от ответственности являются стихийные бедствия, беспорядки, гражданские волнения, восстания, войны, террористические акты, кибератаки или любые забастовки или локауты или любые другие причины, включая отказ оборудования, программного обеспечения или коммуникационной сети, чуму, эпидемию, стихийное бедствие или экстремальное природное явление вне их контроля [6]. Продавец (или другой Бенефициар) после возобновления своей деятельности по-прежнему несут ответственность за выполнение любых обязательств, которые наступили во время такого прекращения деятельности, в течение тридцати (30) календарных дней после такого возобновления.

Положения ст. 17 о применимом праве значительно отличаются от аналогичных положений в Типовом контракте международной купли-продажи товаров. Во-первых, подчеркивается, что применимое право должно соответствовать условиям Цифровой торговой транзакции. URDTT дополняет выбор применимо-

го права, согласованный между Основными сторонами, в той мере, в какой это не запрещено и не противоречит применимому праву или любому применимому регулированию.

Важное значение имеет специальное указание на нормы непосредственного применения (сверхимперативные нормы) применимого права. В п. 3 ст. 17 установлено, что Основная сторона или Поставщик финансовых услуг или любой другой Бенефициар не обязаны соблюдать свои обязательства по Цифровой торговой транзакции, Платежному обязательству или Платежному обязательству FSP и не несут никакой ответственности за какие-либо последствия в отношении такого несоблюдения в той мере, в какой это запрещено применимым правом. Обычно в коммерческих контрактах, включая Типовой контракт ICC международной купли-продажи товаров, прямое указание о таких нормах отсутствует, так как их применение осуществляется в рамках применимого права.

Таким образом можно констатировать, что цифровизация получила дальнейшее закрепление в сфере реализации международных коммерческих контрактов и осуществления платежей по ним, что полностью отвечает современным тенденциям развития.

Список литературы

1. Вилкова Н. Г. Цифровые технологии и международный арбитраж // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции. 23 сентября 2022 г. Казань. В 6 т. Т. 2 / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. Казань, 2023. С. 389-396.

2. Типовой закон ЮНСИТРАЛ об электронной торговле принят 12 июня 1996 г. Законодательство, разработанное на основе или под влиянием Типового закона, принято в общей сложности в 63 юрисдикциях в 83 государствах. URL: https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_commerce

3. Типовой закон ЮНСИТРАЛ об электронных подписях 2001 г. Законодательство, разработанное на основе или под влиянием Типового закона, принято в общей сложности в 38 государствах. URL: https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_signatures

4. Конвенция ООН об использовании электронных сообщений в международных договорах, принята в 2005 г. В конвенции участвует 18 государств, включая Российскую Федерацию, которая ратифицировала конвенцию в январе 2014 г. с двумя оговорками. URL: https://uncitral.un.org/ru/texts/ecommerce/conventions/electronic_communications

5. Типовой закон ЮНСИТРАЛ об электронных передаваемых записях принят в 2017 г. Законодательство на основе Типового закона или под его влиянием принято в 7 государствах. URL: https://uncitral.un.org/ru/texts/ecommerce/modellaw/electronic_transferable_records

6. Рекомендательная оговорка Международной торговой палаты о форс-мажоре принята Палатой в марте 2020 г. URL: https://iccwbo.org/news-publications/icc-rules-guidelines/icc-force-majeure-and-hardship-clauses/

З. У. Гасанов,
кандидат юридических наук, доцент,
Казанский инновационный университет
имени В. Г. Тимирясова

УСИЛЕННАЯ КВАЛИФИЦИРОВАННАЯ ЭЛЕКТРОННАЯ ПОДПИСЬ КАК ФОРМА СОСТАВЛЕНИЯ ЗАВЕЩАНИЯ В УСЛОВИЯХ ЧРЕЗВЫЧАЙНЫХ ОБСТОЯТЕЛЬСТВ: СРАВНИТЕЛЬНО-ПРАВОВОЙ АНАЛИЗ

Аннотация. Статья посвящена применению усиленной квалифицированной электронной подписи в наследственных правоотношениях, а именно наследованию по завещанию, в котором подробно исследуется форма и порядок совершения завещания в чрезвычайных обстоятельствах. Ставится вопрос об использовании усиленной квалифицированной электронной подписи. Обоснована необходимость дифференциации совершения завещания в чрезвычайных обстоятельствах на две категории: 1) составление завещания в чрезвычайных обстоятельствах без использования усиленной квалифицированной электронной подписи; 2) составление завещания в чрезвычайных обстоятельствах с использованием усиленной квалифицированной электронной подписи в присутствии свидетелей и без присутствия свидетелей. Исходя из сформировавшейся в доктрине российской цивилистики позиции о применении усиленной квалифицированной электронной подписи, сделан вывод о необходимости детальной разработки нормативно-правового регулирования совершения завещаний в чрезвычайных обстоятельствах с учетом современных реалий, нуждающихся в цифравизации правового института завещания.

Ключевые слова: электронная подпись, усиленная квалифицированная электронная подпись, наследование по завещанию, завещания в чрезвычайных обстоятельствах, цифровые технологии, роль нотариуса, мобильное приложение

ENHANCED QUALIFIED ELECTRONIC SIGNATURE AS A FORM OF WILLING IN EMERGENCY CIRCUMSTANCES: COMPARATIVE LEGAL ANALYSIS

Abstract. The article is devoted to the use of an enhanced qualified electronic signature (EQES) in hereditary legal relations, namely inheritance by will, which examines in detail the form and procedure for making a will in emergency circumstances. The author raises the question of the use of EQES. The author substantiates the need to differentiate the making of a will in emergency circumstances into two categories: 1) making a will in emergency circumstances without using the EQES; 2) making wills in emergency circumstances using the EQES in the presence of witnesses and without the presence of witnesses. Based on the position formed in the doctrine of Russian civil law on the application of the EQES, the author concludes that it is necessary to develop in detail the legal regulation of making wills in emergency circumstances, taking into account modern realities that need to be digitized as a legal institution of a will.

Keywords: electronic signature, enhanced qualified electronic signature, testamentary inheritance, emergency wills, digital technologies, role of a notary, mobile application

Дмитрий Иванович Мейер, давая определение завещания, указывал, что «духовное завещание… есть удовлетворяющее известным законным условиям изъявление воли лица относительно судьбы его имущественных отношений в случае смерти» [2. С. 1387].

В силу развития цифровизации и права, современных технологий сети Интернет, формирования массивных информационных баз данных, трансформации и широкого внедрения цифровых технологий в общественные массы, деятельность общественных, социальных и, конечно, правовых институтов прогнозируется необходимость цифровизационной динамики и в области наследственных правоотношений.

В современных реалиях представляется необходимым включение способа оформления завещания с использованием цифровых технологий, как одну из возможных и приемлемых волеизъявлений завещателя (то есть электронное завещание), а именно в завещание в чрезвычайных обстоятельствах путем формы усиленной электронной подписи), быть точнее – Усиленная квалифицированная электронная подпись (далее – УКЭП), так как существуют различные виды электронной подписи.

Что же такое УКЭП? Такая подпись является самой надежной и автоматически приравнивается к собственноручной согласно Федеральному закону «Об электронной подписи» от 06.04.2011 (Далее – 63-ФЗ). Такая сила усиленной квалифицированной электронной подписи обусловлена тем, что она выдается аккредитованным удостоверяющим центром, и каждая такая подпись имеет квалифицированный сертификат, выданный им [1. С. 385].

Усиленная квалифицированная электронная подпись– максимально защищенная электронная подпись (далее – ЭП). Ее тоже генерируют в различных программах криптозащиты: в усиленой неквалифицированной электронной подписи сочетают закрытый и открытый ключи. У УКЭП есть несколько отличий от УНЭП: у квалифицированной электронной подписи (далее – КЭП) есть бумажный или электронный квалифицированный сертификат (Приказ ФСБ № 795 от 27.12.2011); программы для КЭП сертифицирует ФСБ; КЭП выдают удостоверяющие центры Федеральной налоговой службы, Федерального казначейства, Центробанка и коммерческие УЦ, аккредитованные Минкомсвязи по особым правилам. УКЭП делает подписанный электронный документ юридически значимым: у простой электронной подписи и неквалифицированной электронной подписи таких возможностей нет. Если подписали документы УКЭП, не надо дополнительно согласовывать и подтверждать их юридический статус с контрагентом.

В 63-ФЗ разрешение или запрет на передачу ЭП прямо не прописан. Но в законе есть другое положение: ключ ЭЦП нельзя использовать без согласия его владельца (п. 1 ст. 10 63-ФЗ). Передавать личную подпись посторонним не рекомендуется. Ключ выдают на конкретное физическое лицо. Это как паспорт: он

принадлежит конкретному владельцу, и другие лица не смогут воспользоваться вашим документом.

То есть завещатель может распорядиться усиленной электронной подписью.

На телефоне нельзя создать юридически значимую ЭП. УКЭП выпускают в удостоверяющем центре ФНС или в аккредитованных УЦ: такая подпись обязательно защищается криптошифрованием. Но вы сможете сделать, например, на айфоне факсимильную подпись, которая воспроизводит собственноручную в цифровом виде. Для этого надо найти инструмент «Разметка» в нужном приложении – «Почта», «Заметки», «Файлы» и др. Инструкция по созданию подписи в телефоне: Откройте нужный pdf-файл. Нажмите значок «Разметка» в правом верхнем углу. Нажмите + на появившейся панели инструментов и выберите «Подпись». Распишитесь пальцем или стилусом на экране. Нажмите «Готово». В результате цифровой автограф появится на документе, но его надо передвинуть в нужное место. При необходимости измените размер или цвет при помощи инструментов в приложении.

Примечательно, что в нескольких штатах США, а также в ряде странах, таких как Франция, Италия, Испания, Мальта, допустимо напечатать завещание или даже использовать современные технические устройства [5. С. 6].

В частности, в Дании законодательством допускается использование современных информационных технологий при составлении завещаний при особых обстоятельствах. Любое выражение последней воли наследодателя может быть составлено в виде текста, записи на магнитной ленте, видео, в электронной почте, на мобильном телефоне или других средствах электронной связи [3. С. 45].

В Тайване же законодателем предусмотрена возможность составления завещания с помощью звукозаписи слов завещателя на магнитофон в присутствии свидетелей.

Интересен опыт Китая, где законодательством предусмотрена как устная форма завещания, так и завещание в виде звукозаписи, которое при этом не связано с наличием каких-либо особых, чрезвычайных обстоятельств.

По мнению Е. Путилина, для такой категории лиц закрытое завещание, совершенное посредством видеозаписи, в большей степени позволило бы определить, в каком состоянии находился завещатель в момент его совершения (совершения записи), и в то же время избежать ущемления прав отдельных граждан на совершение закрытого завещания [4. С. 39].

Рассматривая завещания, составленные в чрезвычайных обстоятельствах, в соответствии с ГК Р.Ф ст.1124, считаем целесообразным изменить ст. 1124 ГК РФ, дополнить ст. 1129 ГК РФ о возможности использования технических и иных средств при составлении завещания в чрезвычайных обстоятельствах (с помощью УКЭП создании единого приложения на базе учетной записи единого портала Госуслуг РФ).

Важно отметить отсутствие четкого понятия «чрезвычайное обстоятельство», что является также почвой для дальнейших исследований. Существует только понятие «чрезвычайная ситуация» в соответствии с ФЗ-68, и, следовательно, назревает необходимость заменить терминологию «чрезвычайные обстоятельства» в сфере наследственных правоотношений на понятие «чрезвычайная ситуация».

Помимо этого, в Методических рекомендациях по удостоверению завещаний и наследственных договоров, утвержденным решением Правления Федеральной нотариальной палаты от 02.03.2021, протокол № 03/21, также следует создать положения о возможности составления завещания с использованием технических средств, а именно УКЭП.

Анализируя статью 1124 ГК РФ, определяя форму завещания, хотелось бы остановиться на исследовании именно завещания в чрезвычайных обстоятельствах.

Аргументируя данное положение, на наш взгляд, необходимо дифференцировать завещания в чрезвычайных обстоятельствах на две категории:

– составление завещания в чрезвычайных обстоятельствах без использования цифровых технологий и с обязательным участием свидетелей;

– составление завещания в чрезвычайных обстоятельствах с использованием цифровых технологий в присутствии свидетелей и без присутствия свидетелей.

То есть полностью придать возможность завещателю «изъявить свою волю», что будет соответствовать принципу свободы завещания.

При определении вышеназванных групп существует необходимость разграничения и строгой дифференциации обстоятельств, при которых составление электронного завещания носило или могло носить единственную возможность выражения воли завещателя, как в присутствии свидетелей, так и без их присутствия.

Одним из ярких тому примеров может послужить произошедшее в феврале 2023 года в Турции землетрясение, в результате которого десятки тысяч жителей, оказавшись лицом к лицу со смертью, вероятно, хотели бы выразить свою последнюю волю каким бы то ни было способом, не имея возможности ни коммуникации с уполномоченными к удостоверению завещания лицами, ни со свидетелями и т. д.

Так, житель одного из разрушенных зданий в провинции Хатай, оказавшись под завалами разрушенного дома, имел в руках лишь одно мобильное устройство. Воспользовавшись этим, он, анализируя ситуацию, явно угрожающую ему смертью, нашел единственно верное решение – записать видеообращение, выражающее его последнюю волю, т. е. составил электронное завещание [6].

На наш взгляд, необходимо учитывать насколько невозможным является признание действительным такого способа составления завещания.

Необходимо разграничивать обстоятельства, в которых представлялось или не представлялось возможным соблюсти ни письменную форму завещания, ни требования нотариального удостоверения, ни привлечения свидетелей.

Подлинность проведения всех данных процедур с использованием цифровых технологий, иначе говоря, удостоверение принадлежности Электронной подписи, следует рассматривать и разрешать по существу в порядке судебного разбирательства, что не исключается (п. 3 ст. 1129 ГК РФ).

Так как выполнение ряда требований не всегда представляется возможным, в частности в Постановлении Пленума Верховного суда от 29.05.2012 № 9 (п. 27), где предписано обязательное участие свидетелей, представляется необходимым внесение дополнения о состоятельности тех завещаний, которые были составлены в условиях чрезвычайных обстоятельств с невозможностью привлечения свидетелей.

В заключение хотелось бы сказать, что, несмотря на прогрессивное развитие отечественного гражданского законодательства, вопросам составления завещаний в чрезвычайных обстоятельствах законодателем, на наш взгляд, придается недостаточное значение. Последними изменениями был дополнен лишь п. 4 ст. 1129 ГК РФ о совместном завещании супругов, наследственных договорах, но форма и порядок совершения завещания не были изменены. Учитывая имеющиеся в связи с новыми событиями обстоятельства и растущую тенденцию к цифровизации современного общества, наблюдается необходимость детально разработать наследственные вопросовы на законодательном уровне, дать возможность завещателю максимально свободно и доступно придать юридическую форму своей воле.

Список литературы

1. Кодификация российского частного права / В. В. Витрянский, С. Ю. Головина, Б. М. Гонгало и др.; под ред. Д. А. Медведева. М.: Статут, 2019.

2. Мейер Д. И. Русское гражданское право. М.: Статут, 2003.

3. Паничкин В. Б. Различие завещания в российском и англо-американском праве и их правовая природа // Нотариус. 2019. № 2. С. 45.

4. Путилина Е. Совершение закрытого завещания и завещания в чрезвычайных обстоятельствах // Законность. 2007. № 11. С. 39-45.

5. Bennet M. Technology and Wills (Using an iPhone, Word or Other Modern Devices) // Lexology. 2020. P. 6.

6. Enkazın altında Son videom' diye çekti. URL: https://www.cnnturk.com/video/turkiye/enkazin-altinda-son-videom-diye-cekti

Е. Н. Гладкая,
кандидат юридических наук,
Институт экономики Национальной академии наук Беларуси

КРИПТОАКТИВЫ КАК ОБЪЕКТЫ ГРАЖДАНСКОГО ПРАВА: ПОСТАНОВКА ПРОБЛЕМЫ И ПУТИ РЕШЕНИЯ В КОНТЕКСТЕ ГАРМОНИЗАЦИИ ПРАВОВОГО РЕГУЛИРОВАНИЯ НА ТЕРРИТОРИИ ГОСУДАРСТВ – ЧЛЕНОВ ЕАЭС

Аннотация. В статье на основании доктринальных подходов и рекомендаций Евразийской экономической комиссии по определению правовой и экономической сущности криптоактивов, а также результатов сравнительного анализа законодательств государств-членов ЕАЭС в криптосфере, выработаны предложения, направленные на гармонизацию правового регулирования криптоотношений на территории стран региональной экономической интеграции с целью адекватного реагирования на современные вызовы и угрозы.

Ключевые слова: гражданское право, объекты гражданских прав, имущество, имущественные права, цифровые активы, цифровые финансовые активы, виртуальные активы, цифровые токены, криптовалюта

CRYPTOASSETS AS OBJECTS OF CIVIL LAW: STATEMENT OF THE PROBLEM AND WAYS OF SOLUTION IN THE CONTEXT OF HARMONIZATION OF LEGAL REGULATION IN THE TERRITORY OF THE MEMBER STATES OF THE EAEU

Abstract. In the article, based on doctrinal approaches and recommendations of the Eurasian Economic Commission to determine the legal and economic essence of crypto-assets, as well as the results of a comparative analysis of the legislation of the EAEU member states in the cryptosphere, proposals are developed aimed at harmonizing the legal regulation of crypto-relations in the countries of regional economic integration in order to adequately respond to modern challenges and threats.

Keywords: civil law, objects of civil rights, property, property rights, digital assets, digital financial assets, virtual assets, digital tokens, cryptocurrency

Введение. Современные вызовы и угрозы создают предпосылки для актуализации поиска решения вопросов, касающихся гармонизации законодательств государств – членов ЕАЭС в различных сферах правового регулирования. В качестве одной из важнейших таких сфер представляется криптосфера. Будучи новыми и востребованными, объекты криптосферы широко используются различными субъектами общественных отношений. Полагаем, что с течением времени количество областей применения таких объектов будет только увеличиваться. Вместе с тем следует констатировать, что до настоящего времени в законодательствах государств – членов ЕАЭС не выработано единого терминологического аппарата, позволяющего разграничить объекты криптосферы, определить правовой статус и правовой режим таких объектов, а значит, и их место среди иных объектов общественных отношений и объектов гражданских прав, в частности. Справедливости ради необходимо отметить, что такого рода тенденция характерна не только для стран региональной экономической интеграции, что отмечается в трудах зарубежных ученых.

На основании вышеуказанного была сформулирована цель настоящего исследования – выработать предложения по гармонизации законодательств государств – членов ЕАЭС в криптосфере. Для достижения обозначенной цели были поставлены следующие задачи:

1) изучить доктринальные подходы в области определения правовой и экономической сущности криптоактивов;

2) проанализировать рекомендации Евразийской экономической комиссии (далее – ЕЭК) в части определения правового статуса и правового режима объектов криптосферы;

3) рассмотреть подходы к определению правового статуса и правового режима объектов криптосферы в законодательстве государств-членов ЕАЭС;

4) на основании полученных результатов выработать предложения, направленные на гармонизацию законодательств государств-членов в исследуемой сфере.

Основная часть. В настоящее время законодательство Республики Беларусь не содержит понятия «криптоактивы». В отечественной научной литературе также

не выработано унифицированного определения данным объектам общественных отношений. Белорусские ученые в своих трудах преимущественно используют уже ставшие привычными понятия «токен», «криптовалюта» и другие, т. е. те, что прямо следуют из законодательства Республики Беларусь, в частности из Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» [16] (далее – Декрет № 8 «О развитии цифровой экономики»). В зарубежной научной литературе по вопросу понятия криптоактивов высказаны различные точки зрения. Приведем некоторые из них.

В. Е. Понамаренко, Д. В. Дибина отмечают, что статус криптоактивов на территории Российской Федерации определен в Федеральном законе от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации») [18]. Анализируя содержание указанного закона, ученые делают заключение, что, согласно его положениям, под криптоактивами следует понимать цифровую валюту. Так, по их мнению, «Особый подход в регулировании криптоактивов прослеживается уже в вопросе терминологии: российский законодатель вместо широкоупотребительных в цифровой среде терминов «виртуальные активы» (ФАТФ), «криптоактивы» (ЕС), «цифровые активы» (США, иные страны) использует термин «цифровая валюта»» [19]. Данная точка зрения представляется спорной, поскольку, помимо цифровых валют, в ст. 1 ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» предметом правового регулирования также признаются цифровые финансовые активы.

Я. К. Ярутин, Е. Е. Гуляева в своей статье «Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция» приводят понятие криптоактивов, сформулированное Советом по финансовой стабильности. В соответствии с ним под криптоактивами необходимо понимать отображение ценности в цифровом виде (digital representation of value), которое основано на криптографии и технологии распределенного реестра (Distributed Ledger Technology, DLT), аналогичных технологиях и которое может использоваться как в платежных, так и в инвестиционных целях [23. С. 728]. Отдельно ими отмечено, что данным понятием не охватывается цифровое отображение фиатных валют [23. С. 729].

Руководствуясь приведенным понятием криптоактивов, Я. К. Ярутин, Е. Е. Гуляева вносят предложение о замене понятия «цифровые финансовые активы», использованного в ст. 1 ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», на «криптоактивы». Понятие «цифровая валюта» ученые считают необходимым упразднить и в дальнейшем использовать понятие «цифровая валюта центрального банка» [23. С. 738–739].

М. В. Савельева к признакам криптоактивов относит: нематериальность; криптографическую аутентификацию; использование распределенного реестра

транзакций; децентрализацию; правила реестра (правила консенсуса), установленные участниками оборота; виртуальность; оборотоспособность; экстерриториальность и приходит к выводу, что под последними следует понимать активы, защищенные криптографическим методом, и включающие две группы объектов: криптовалюты (crypto currency) и токены (tokens) [20. С. 81, 84]. Следует отметить, что в более ранних трудах М. В. Савельева указывала на невозможность выработки определения криптоактивов, но делала заключение о том, что «криптоактив включает в себя криптовалюты, является разновидностью цифровых прав (rights digital), частично может совпадать по содержанию с цифровыми финансовыми активам» и шире определения цифровых прав данных в ст. 141.1 ГК РФ» [21. С. 169].

Приведенные точки зрения указывают на отсутствие единства мнений по вопросу определения сущности криптоактивов среди юридического научного сообщества. Для полноты исследования обратимся к изучению наработок ученых-экономистов в обозначенной области.

Л. В. Волкова предлагает под криптоактивом понимать «ресурс нематериальной формы, отражающий наличие определенной ценности или определенных юридических прав, обеспечивающий сохранение информации о таких правах или ценности с помощью криптотехнологии и технологии дублирования данных по различным узлам и серверам независимыми между собой участниками» [3. С. 16]. К преимуществам данного определения ученый относит нивелирование внимания от эмитентов криптоактивов, акцент на значительное количество независимых участников и дублирование серверов и узлов поддержки системы.

Д. А. Кочергин, Н. В. Покровская выделяют ряд проблем, существующих в области определения сущности криптоактивов. Среди них ученые отмечают: отсутствие унифицированного термина «криптоактивы» как нового класса финансовых активов; неопределенность среди экономистов и финансовых регуляторов в решении вопроса о том, какие именно типы активов могут относиться к криптоактивам и по каким критериям они сущностно отличаются друг от друга; различия в подходах к интерпретации и классификации криптоактивов между странами [10. С. 184]. Выделенные проблемы обуславливают появление новых. Так, ученые указывают, что в различных странах предпринимаются попытки налогообложения операций, связанных с криптоактивами, вместе с тем их теоретическое обоснование, как правило, следует за практикой их применения.

С целью решения обозначенных выше проблем Д. А. Кочергин, Н. В. Покровская предлагают к использованию авторское определение криптоактивов. Согласно ему, криптоактивы – это «<…> частные цифровые активы, которые: 1) записываются в цифровой форме в каком-либо распределенном реестре, защищенном криптографически; 2) не выпускаются и не гарантируются Центральным банком или государственными органами власти; и 3) могут использоваться в качестве средства обмена, и/или для инвестиционных целей, и/или для доступа к товару или услуге» [10. С. 187].

Т. А. Степанова, Л. Н. Измайлова, А. В. Воронина предлагают авторскую типизацию криптоактивов. В соответствии с ней ученые выделяют три типа крипто-

активов: криптовалюты, токены (токены аналогичные акциям, токены полезности, токены безопасности), криптоактивы смешанного типа [22. С. 284–285].

Результаты исследования, проведенного коллективом авторов в составе T. Ankenbrand, D. Bieri, R. Cortivo, J. Hoehener and T. Hardjono, направленного на таксономию криптовалютных активов, позволили авторам выделить четырнадцать оснований для классификации последних. В качестве таковых оснований были названы: Claim structure; Technology; Underlying; Consensus/Validation mechanism; Legal status; Governance; Information complexity; Legal structure; Information interface; Total supply; Issuance; Redemption; Transferability; Fungibility [1].

Применение сформулированных оснований для классификации криптовалютных активов позволит, по мнению авторов, «In this way, our taxonomy bridges the gap between physical, digital, and cryptographic assets, <…> thus creating clear terminology» [1], т. е. устранить разрыв между физическими, цифровыми и криптографическими активами, создавая тем самым четкую терминологию.

Как показывают результаты исследования, в настоящее время не сложились единые доктринальные подходы в области определения как правовой, так и экономической сущности криптоактивов. Следует отметить, что такого рода тенденция наблюдается среди ученых не только ближнего, но и дальнего зарубежья. Тем не менее научным сообществом предпринимаются попытки выработки оптимальных решений обозначенной проблемы.

В соответствии со ст. 4 Договора о Евразийском экономическом союзе (далее – Союз) от 29 мая 2014 г. [8] основными целями Союза являются: создание условий для стабильного развития экономик государств-членов в интересах повышения жизненного уровня их населения; стремление к формированию единого рынка товаров, услуг, капитала и трудовых ресурсов в рамках Союза; всесторонняя модернизация, кооперация и повышение конкурентоспособности национальных экономик в условиях глобальной экономики. Для достижения обозначенных целей по направлению криптовалют и технологии блокчейн в 2019 г. Евразийской экономической комиссией был подготовлен доклад «Криптовалюты и блокчейн как атрибуты новой экономики. Разработка регуляторных подходов: международный опыт, практика государств – членов ЕАЭС, перспективы для применения в Евразийском экономическом союзе» [9] (далее – доклад ЕЭК). Согласно содержанию указанного доклада, с целью гармонизации подходов государств – членов ЕАЭС к регулированию сферы криптовалют и блокчейн было предложено утвердить Единый глоссарий, содержащий основные термины и определения в сфере криптовалют и блокчейн, а также принципы государственного регулирования данной сферы. В качестве последних были названы такие принципы, как:

1. единое понимание и толкование основных терминов и понятий, связанных с использованием цифровых активов, цифровых знаков (токенов), криптовалют;

2. соблюдение баланса между контролем рисков и реализацией инновационных стимулов экономического развития, в том числе:

2.1. обеспечение транспарентности и гибкости регуляторной среды государств-членов в целях привлечения инвестиций и снижения масштабов теневых сделок;

2.2. защита прав профессиональных и непрофессиональных инвесторов рынка цифровых активов;

2.3. формирование единых подходов к обеспечению информационной безопасности;

2.4. включение саморегулируемых организаций и профессиональных ассоциаций в систему регулирования экономической деятельности в области цифровых активов, цифровых знаков (токенов), криптовалют;

2.5. введение ограничений на оборот цифровых активов, учитывающее последствия таких ограничений как для рынка, так и для правоприменения;

3. гармонизация подходов к регулированию деятельности в области цифровых активов, цифровых знаков (токенов), криптовалют на территории государств – членов ЕАЭС, в т. ч.:

3.1. поэтапное развитие регуляторной практики и необходимой инфраструктуры с учетом динамики и масштабов явления;

3.2. реализация уполномоченными органами практики «мягкого регулирования», включая публикацию предупреждений и разъяснений, повышение грамотности и информированности граждан и организаций;

3.3. обмен эффективными регуляторными практиками для масштабирования на пространстве ЕАЭС;

3.4. разработка единых принципов идентификации пользователей цифровых знаков (токенов);

3.5. стремление к гармонизации подходов к налогообложению операций с цифровыми знаками (токенами) с учетом требований национального законодательства;

4. взаимодействие с третьими странами и международными организациями с целью разработки и применения передовых стандартов регулирования обращения цифровых активов, цифровых знаков (токенов), криптовалют, в т. ч.:

4.1. выполнение международных стандартов в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (ПОД/ФТ);

4.2. обмен информацией о фактах использования цифровых активов в операциях, предположительно связанных с хищениями денежных средств» [9].

В Приложении II к докладу ЕЭК размещен Глоссарий ЕАЭС, в который вошли следующие понятия: цифровой актив, цифровой знак (токен), криптовалюта, цифровой кошелек, оператор цифрового кошелька, майнинг, оператор обмена цифровых знаков (токенов), оператор торговой платформы по обмену цифровых знаков (токенов), распределенная база данных, реестр блоков транзакций (блокчейн), смарт-контракт. В контексте темы исследования уделим внимание некоторым из них (табл. 1).

Таблица 1

Цифровой актив, цифровой знак (токен), криптовалюта в значении, определенном в Глоссарии ЕАЭС (Приложение II к докладу ЕЭК) [9]

№	Термин	Определение	Комментарии к нему
1	Цифровой актив	Имущество в электронной форме, создание и использование которого осуществляется с помощью цифровых технологий	Вводя понятие цифрового актива, регулятор обеспечивает возможность использования существующих норм гражданского права для юридической защиты сделок с различными видами цифрового представления ценностей. Понятие «цифровой актив» используется как более общее родовое понятие для различного рода токенов (продуктовые, имущественные, гибридные) и криптовалют. Данный подход по введению в оборот общего собирательного понятия («зонтичное определение») соответствует практике ОЭСР, согласно которой используется понятие «цифровые финансовые активы». Уточнение «финансовый» в данном случае не применяется, поскольку такая формулировка ограничивает применение определения для нефинансовых токенов
2	Цифровой знак (токен)	Вид цифрового актива, средство удостоверения обязательственных и иных прав, в том числе прав доступа к продуктам или услугам, прав на определенный продукт или услугу, прав на получение фиксированного дохода или процента от прибыли, прав управления, прав на покупку определенного актива по определенной цене в будущем. Может содержать условия смарт-контракта, связанные с удостоверяемыми правами	Вводя отдельное понятие «цифрового знака (токена)», регулятор обеспечивает возможность развития законодательства в сфере процессов так называемой токенизации активов и услуг. В мировой практике используется схожее понятие – «виртуальный токен» (США (SEC)). Сегодня выделяют платежные (payment tokens), пользовательские (utility token) токены, токены-активы (assets tokens), гибридные токены (FINMA, Швейцария). Схожее деление разрабатывает ОЭСР

Окончание табл. 1

№	Термин	Определение	Комментарии к нему
3	Криптовалюта	Вид цифрового знака (токена), представляющий собой запись в реестре блоков транзакций (блокчейне), иной распределенной базе данных и принимаемый в качестве средства обмена и (или) единицы учета и (или) средства хранения (накопления) стоимости	При определении понятия предпочтение отдается определению криптовалюты как цифрового актива вместо платежного средства/денежного суррогата ввиду ограничений национального законодательства, предусматривающего использование в качестве платежного средства исключительно национальной валюты и требующего в таком случае более жесткого регулирования со стороны национальных (центральных) банков. По этой же причине одна из функций криптовалюты обозначена как единица учета вместо расчетной единицы. В мировой практике встречаются схожие понятия: «виртуальная валюта» (ФАТФ, ЕС, США, Эстония, Япония, Швейцария), «цифровая валюта» (Великобритания). Использование данных понятий нежелательно в силу своей стилистической окраски: «цифровой», «виртуальный». Понятие «криптовалюта» является общепринятым в профессиональной среде, отражает технологическую сторону данного явления: результат соединения криптографических технологий и технологии распределенных реестров, позволяющий за счет этого обеспечивать выполнение отдельных функций традиционных денежных средств

Соответственно, ЕЭК понятие «цифровой актив» предлагается использовать как понятие собирательное (зонтичное), под которым следует понимать любое имущество в электронной форме, созданное и используемое с помощью цифровых технологий. В свою очередь цифровой знак (токен) определяется как вид цифрового актива, криптовалюта – как вид цифрового знака (токена). Таким образом, соотношение указанных понятий в предложенных формулировках можно представить в следующем виде (рис. 1).

Принимая во внимание вышеуказанное, полагаем, что не будет ошибочным утверждение о том, что понятие «цифровой актив» в значении, сформулированном в докладе ЕЭК, можно считать синонимом понятия «криптоактив».

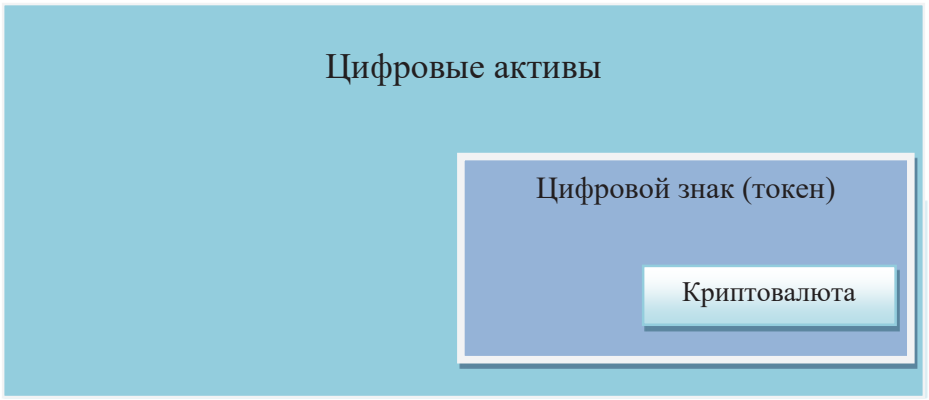

Рис. 1. Соотношение понятий цифровой актив, цифровой знак (токен), криптовалюта в значении, определенном в Глоссарии ЕАЭС (Приложение II к докладу ЕЭК)

Примечание: является авторской разработкой.

Несмотря на взятый курс на гармонизацию подходов к регулированию деятельности в области цифровых активов, цифровых знаков (токенов), криптовалют на территории государств – членов ЕАЭС и выработку единого понимания и толкования основных терминов и понятий, связанных с их использованием, до настоящего времени указанные цели достигнуты не были.

Как указывалось, в Российской Федерации основным нормативным правовым актом, регулирующим отношения, объектом которых выступают криптоактивы, является ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». В соответствии с п. 1 ст. 1 данного закона, предметом его правового регулирования выступают общественные отношения, возникающие при выпуске, учете и обращении цифровых финансовых активов, особенности деятельности оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов, и оператора обмена цифровых финансовых активов, а также отношения, возникающие при обороте цифровой валюты в Российской Федерации.

Следовательно, объектами правового регулирования вышеупомянутого закона являются цифровые финансовые активы и цифровые валюты. Понятия указанных объектов содержатся в п. 2, 3 ст. 1 ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». Согласно п. 2 ст. 1 закона, цифровыми финансовыми активами признаются цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном указанным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы.

Справочно: правовая природа цифровых прав определена в ст. 128, 141.1 Гражданского кодекса Российской Федерации [7] (далее – ГК Российской Федерации). Так, ст. 128 ГК Российской Федерации цифровые права, наряду с безналичными денежными средствами (в том числе цифровыми рублями) и бездокументарными ценными бумагами, отнесены к имущественным правам. Согласно ст. 141.1 ГК Российской Федерации, цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам.

В соответствии с п. 3 ст. 1 ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», цифровой валютой признается совокупность электронных данных (цифрового кода или обозначения), содержащихся в информационной системе, которые предлагаются и (или) могут быть приняты в качестве средства платежа, не являющегося денежной единицей Российской Федерации, денежной единицей иностранного государства и (или) международной денежной или расчетной единицей, и (или) в качестве инвестиций и в отношении которых отсутствует лицо, обязанное перед каждым обладателем таких электронных данных, за исключением оператора и (или) узлов информационной системы, обязанных только обеспечивать соответствие порядка выпуска этих электронных данных и осуществления в их отношении действий по внесению (изменению) записей в такую информационную систему ее правилам. Понятие «цифровая валюта» в ГК Российской Федерации отсутствует.

Как видим, в законодательстве Российской Федерации сформировался отличный от предложенного ЕЭК подход к определению сущности криптообъектов. Цифровые активы здесь рассматриваются исключительно с приставкой «финансовые» и как объекты гражданского права отнесены к имущественным правам.

В Республике Казахстан принят Закон от 25 июня 2020 г. № 347-VI «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий» [14]. На его основании были внесены изменения в Гражданский кодекс Республики Казахстан (Общая часть) [6] (далее – ГК Республики Казахстан) и Закон Республики Казахстан от 24 ноября 2015 г. № 418-V «Об информатизации» [11] (далее – Закон Республики Казахстан «Об информатизации»). В частности, п. 2 ст. 115 ГК Республики Казахстан был дополнен новым видом имущества – цифровыми активами. Понятия «цифровой актив», «цифровой майнинг», «цифровой токен» и другие нашли свое отражение в Законе Республики Казахстан «Об информатизации».

С принятием Закона Республики Казахстан от 6 февраля 2023 г. № 193-VII «О цифровых активах в Республике Казахстан» [17] (далее – Закон Республики Казахстан «О цифровых активах в Республике Казахстан») начался новый этап развития общественных отношений, основанных на использовании цифровых активов, в данной республике. В соответствии со ст. 1 указанного закона было уточнено понятие «цифровой актив», дано определение понятиям «обеспеченный цифровой актив» и «необеспеченный цифровой актив» и другое. Так, было установлено,

что цифровой актив – это имущество, созданное в электронно-цифровой форме с присвоением цифрового кода, в том числе с применением средств криптографии и компьютерных вычислений, зарегистрированное и обеспеченное неизменностью информации на основе технологии распределенной платформы данных; обеспеченный цифровой актив – цифровой актив, зарегистрированный посредством цифровой платформы по хранению и обмену обеспеченными цифровыми активами, который удостоверяет права на материальные, интеллектуальные услуги и активы, за исключением денег и ценных бумаг; необеспеченный цифровой актив – цифровой актив, полученный в информационной системе в виде вознаграждения за участие в поддержании консенсуса в блокчейне и не выражающий чьи-либо денежные обязательства, которыми можно торговать в цифровой форме на бирже цифровых активов. В силу п. 5 ст. 11 Закона Республики Казахстан «О цифровых активах в Республике Казахстан» на территории Республики Казахстан запрещаются выпуск и оборот необеспеченных цифровых активов, а также деятельность бирж цифровых активов по необеспеченным цифровым активам, за исключением территории Международного финансового центра «Астана». Примером необеспеченных цифровых активов служат криптовалюты.

Отметим, что в ст. 1 Закона Республики Казахстан «О цифровых активах в Республике Казахстан» отсутствует понятие «цифровой токен». Законом Республики Казахстан от 6 февраля 2023 г. № 194-VII «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровых активов и информатизации» [15] понятие «цифровой токен» исключено из Закона Республики Казахстан «Об информатизации».

Анализ законодательства Республики Казахстан в части правового регулирования деятельности с цифровыми активами позволяет сделать вывод о том, что сформированный в данной республике подход соответствует рекомендациям ЕЭК, но вместе с тем имеет описанные выше отличительные признаки.

В отличие от законодательств вышеуказанных стран в законодательстве Кыргызской Республики вместо понятия «цифровые активы» используется понятие «виртуальные активы». Так, Законом Кыргызской Республики от 21 января 2022 г. № 12 «О виртуальных активах» [12] (далее – Закон Кыргызской Республики «О виртуальных активах») установлено, что виртуальные активы представляют собой совокупность данных в электронно-цифровой форме, имеющую стоимость, являющуюся цифровым выражением ценности и/или средством удостоверения имущественных и/или неимущественных прав, которая создается, хранится и обращается с использованием технологии распределенных реестров или аналогичной технологии и не является денежной единицей (валютой), средством платежа и ценной бумагой (п. 1 ст. 4 закона). Статьей 5 Закона Кыргызской Республики «О виртуальных активах» определен правовой статус виртуальных активов. В соответствии с ней виртуальный актив может быть как самостоятельным объектом гражданского права, так и средством удостоверения имущественных и (или) неимущественных прав, в том числе прав требования на другие объекты гражданских прав. Виртуальные активы не являются платежным средством, валютой и (или) ценной бумагой на территории Кыргызской Республики. Виртуальные активы

могут быть обеспеченными (цифровые токены, иные виртуальные активы, обеспеченные другими объектами гражданских прав) или необеспеченными (виртуальные активы, в отношении которых отсутствует лицо (лица), несущее обязательства перед каждым обладателем таких виртуальных активов). Следовательно, в законодательстве Кыргызской Республики понятие «цифровой токен» сохранено. В силу п. 1 ст. 4 Закона Кыргызской Республики «О виртуальных активах», под цифровым токеном необходимо понимать вид виртуального актива, являющийся средством удостоверения имущественных и (или) неимущественных прав, в том числе прав требования на другие объекты гражданских прав.

Законом Кыргызской Республики от 5 августа 2022 г. № 81 «О внесении изменений в некоторые законодательные акты в сфере виртуальных активов» [13] внесены изменения в ст. 22 «Виды объектов гражданских прав» части I Гражданского кодекса Кыргызской Республики [4]. Согласно им, указанная статья была дополнена виртуальными активами, которые наряду с вещами были отнесены к имуществу.

Республика Армения – единственная среди государств – членов ЕАЭС, в которой нет нормативного правового акта, регулирующего деятельность с использованием цифровых активов. Вместе с тем экспертное сообщество Республики Армения активно работает над предложениями по созданию конкурентного нормативного правового регулирования данной сферы. Так, президент Армянской блокчейн ассоциации «Nooor» В. Арушанян в своем интервью отметил: «Мы в Nooor разработали и представили законопроект, который сейчас рассматривается правительством. В случае его принятия Армения станет одной из самых привлекательных юрисдикций для блокчейн-проектов в мире» [2].

Как отмечалось выше, в Республике Беларусь основу правового регулирования криптосферы составляет Декрет № 8 «О развитии цифровой экономики». Принятый в 2017 г. указанный нормативный правовой акт был прорывным для своего времени. Установив экспериментальный правовой режим для новых объектов гражданских прав (выступив регуляторной песочницей), Декрет № 8 «О развитии цифровой экономики был призван решить ряд проблемных вопросов, возникших в связи с появлением технологии блокчейн и криптовалют.

В приложении 1 к Декрету № 8 «О развитии цифровой экономики» размещен перечень используемых терминов и их определений. В соответствии с ним под криптовалютой понимается биткоин, иной цифровой знак (токен), используемый в международном обороте в качестве универсального средства обмена. Под цифровым знаком (токеном) – запись в реестре блоков транзакций (блокчейне), иной распределенной информационной системе, которая удостоверяет наличие у владельца цифрового знака (токена) прав на объекты гражданских прав и (или) является криптовалютой. В этот же перечень включено понятие «владелец цифрового знака (токена)», под которым следует понимать субъекта гражданского права, которому цифровой знак (токен) принадлежит на праве собственности или на ином вещном праве. Таким образом, согласно установленному Декретом № 8 «О развитии цифровой экономики» экспериментальному правовому режиму, цифровой знак (токен) в белорусском законодательстве признается объектом вещных прав, а значит, и объектом гражданских правоотношений.

Требуется отметить, что ни в Декрете № 8 «О развитии цифровой экономики», ни в белорусском законодательстве в целом понятие «цифровой актив» (как и «криптоактив», «виртуальный актив») не используется.

С момента принятия Декрета № 8 «О развитии цифровой экономики» прошло достаточно много времени и, по нашему мнению, требуется и дальше развивать белорусское законодательство в криптосфере. Так, видится необходимым отойти от экспериментального правового режима регулирования отношений, основанных на использовании цифровых токенов и криптовалюты. Для этого необходимо:

1) расширить перечень объектов правового регулирования за счет включения в него цифровых активов. В дальнейшем указанное понятие использовать как «зонтичное»;

2) принять во внимание рекомендации ЕЭК в части разграничения понятий «цифровой актив», «цифровой знак (токен)», «криптовалюта»;

3) определить правовой статус и правовой режим указанных объектов как объектов гражданских прав путем внесения соответствующих изменений в ст. 128 Гражданского кодекса Республики Беларусь;

4) разработать и принять отдельный нормативный правовой акт (закон), регулирующий общественные отношения, складывающиеся по поводу цифровых активов, на территории Республики Беларусь.

Заключение. На основании проведенного исследования можно сделать следующие выводы:

1) понятие «криптоактивы» выступает исключительно доктринальным. Вместе с тем оно синонимично понятиям «цифровые активы», «виртуальные активы»;

2) в качестве «зонтичного» понятия применительно к объектам криптосферы в законодательстве государств – членов ЕАЭС предлагается использовать понятие «цифровые активы» в значении, определенном в докладе ЕЭК, что будет первым шагом на пути гармонизации законодательства стран региональной экономической интеграции в указанной сфере;

3) вторым шагом видится формулирование единых подходов в области определения правового статуса и правового режима цифровых активов в законодательствах государств – членов ЕАЭС;

4) применительно к законодательству Республики Беларусь в контексте темы исследования предлагается отказаться от экспериментального режима правового регулирования криптоотношений. Для это необходимо внести соответствующие изменения в ГК Республики Беларусь и разработать специальный нормативный правовой акт в виде закона, предметом правового регулирования которого станут общественные отношения, складывающиеся по поводу цифровых активов.

Список литературы

1. Ankenbrand T., Bieri D., Cortivo R., Hoehener J. and Hardjono T. Proposal for a Comprehensive (Crypto) Asset Taxonomy // Crypto Valley Conference on Blockchain Technology (CVCBT). 2020. Pp. 16-26.

2. Арушанян В. Нынешнее использование блокчейна – это эволюция, но я ожидаю революцию. URL: https://letknow.news

3. Волкова Л. В. Риски и новые возможности, генерируемые криптоактивами в российской федерации // BENEFICIUM. 2023. № 1(46). С. 14-19.

4. Гражданский кодекс Кыргызской Республики (часть I). URL: http://cbd.minjust.gov.kg/act/view/ru-ru/4?cl=ru-ru#st_22

5. Гражданский кодекс Республики Беларусь. URL: https://etalonline.by

6. Гражданский кодекс Республики Казахстан (Общая часть). URL: https://online.zakon.kz

7. Гражданский кодекс Российской Федерации (часть первая) // СПС «КонсультантПлюс».

8. Договор о Евразийском экономическом союзе от 29.05.2014. URL: https://etalonline.by/document/?regnum=f01400176&q_id=8795942

9. Доклад ЕЭК «Криптовалюты и блокчейн как атрибуты новой экономики. Разработка регуляторных подходов: международный опыт, практика государств-членов ЕАЭС, перспективы для применения в Евразийском экономическом союзе». Москва, 2019. URL: https://eec.eaeunion.org/upload/medialibrary/71f/Doklad_FINAL.pdf

10. Кочергин Д. А., Покровская Н. В. Интерпретация криптоактивов и особенности их налогообложения в развитых странах и России // Вестник Московского университета. Серия 6. Экономика. 2020. № 5. С. 182-215.

11. Об информатизации: Закон Республики Казахстан. URL: https://online.zakon.kz/Document/?doc_id=33885902&pos=1;-8#pos=1;-8

12. О виртуальных активах: Закон Кыргызской Республики. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/112346

13. О внесении изменений в некоторые законодательные акты в сфере виртуальных активов: Закон Кыргызской Республики. URL: http://cbd.minjust.gov.kg/act/view/ru-ru/112417?cl=ru-ru

14. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам регулирования цифровых технологий: Закон Республики Казахстан. URL: https://online.zakon.kz/Document/?doc_id=34230083&show_di=1

15. О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам цифровых активов и информатизации: Закон Республики Казахстан. URL: https://online.zakon.kz/Document/?doc_id=38779038&show_di=1

16. О развитии цифровой экономики: Декрет Президента Республики Беларусь. URL: https://etalonline.by

17. О цифровых активах в Республике Казахстан: Закон Республики Казахстан. URL: https://online.zakon.kz

18. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон // СПС «КонсультантПлюс»

19. Понамаренко В. Е., Дибина Д. В. Правовое регулирование криптоактивов в передовых криптоюрисдикциях Европы: Мальта, Лихтенштейн, Швейцария // Журнал юридических исследований. 2021. Т. 6, № 2.

20. Савельева М. В. О формировании механизма правового регулирования отношений, связанных с криптоактивами, в эпоху глобальной цифровизации // Академический юридический журнал. 2022. Т. 23, № 1. С. 78-86.

21. Савельева М. В. Понятие криптоактива и его место в системе гражданского права // Современные тенденции развития гражданского и гражданского процессуального законодательства и практики его применения. 2021. № 7. С. 163-170.

22. Степанова Т. А., Измайлова Л. Н., Воронина А. В. Регулирование рынка криптоактивов // Russian Economic Bulletin. 2023. Т. 6, № 2. С. 282-288.

23. Ярутин Я. К., Гуляева Е. Е. Международное и российское правовое регулирование оборота криптоактивов: понятийно-терминологическая корреляция // Journal of Digital Technologies and Law. 2023. № 1(3). С. 725-751.

Д. А. Дудкин,
адъюнкт,
Академия управления
Министерства внутренних дел Российской Федерации

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ОКАЗАНИЯ ДЕТЕКТИВНЫХ (СЫСКНЫХ) УСЛУГ КАК ПРЕДМЕТА ДОГОВОРА

Аннотация. В реалиях сегодняшнего времени, в том числе в условиях всеобъемлющей цифровизации общества, вопрос безопасности государства, а также граждан и их имущества в информационном поле и кибепространстве становится особенно острым. На данном этапе развития гражданских правоотношений в области сыска отсутствует всеобъемлющее исследование, которое полностью разбирает суть договора оказания детективных услуг в качестве процесса их предоставления, выражающегося в определенном виде услуг как предмета договора, который все чаще заключается в электронном виде. Чтобы сформулировать вышеназванное понятие, необходимо выявить правовую природу детективных (сыскных) услуг как предмета договора и проследить ее трансформацию.

Ключевые слова: детективная деятельность, детективные (сыскные) услуги, договор оказания детективных услуг, динамика предпринимательской деятельности

DIGITAL TRANSFORMATION OF THE PROVISION OF DETECTIVE (INTESTIGENT) SERVICES AS THE SUBJECT OF THE CONTRACT

Abstract: In the realities of today, including in the conditions of comprehensive digitalization of society, the issue of the security of the state, as well as citizens and their property in the information field and cyberspace is becoming particularly acute. At this stage of the development of civil legal relations in the field of investigation, there is no

comprehensive study that fully explores the essence of the contract for the provision of detective services as a process of their provision, expressed in a certain type of services as the subject of the contract, which is increasingly concluded in electronic form. To formulate the above-mentioned concept, it is necessary to identify the legal nature of detective (detective) services as the subject of the contract and trace its transformation.

Keywords: detective activity, detective (detective) services, contract for the provision of detective services, dynamics of entrepreneurial activity

Согласно ст. 1 Закона РФ «О частной детективной и охранной деятельности в Российской Федерации» [2] (далее – Закон о сыске) частная детективная (сыскная) деятельность (далее – ЧДД) определяется как оказание на возмездной договорной основе услуг физическим и юридическим лицам. На договорную природу взаимоотношений между детективом и его клиентом в том числе указывает ст. 9 этого Закона, поименованная «Особенности требований к договору на оказание сыскных услуг». Так, детектив обязан заключить с каждым из своих клиентов договор на оказание сыскных услуг в письменной форме. Это может быть сделано путем составления одного документа (в том числе электронного), подписанного сторонами, или обмена письмами, телеграммами, электронными документами или другими средствами согласно правилам, установленным в Гражданском кодексе Российской Федерации (далее – ГК РФ). В этом договоре должны быть указаны сведения о сторонах, включая номер и дату выдачи лицензии, вид и содержание оказываемых услуг, срок их оказания, стоимость услуг или метод определения стоимости. С одной стороны, названные элементы подтверждают существенность условий договора, без которых он не может считаться заключенным. В то же время стоит согласиться с С. А. Шароновым в том, что эти элементы нельзя в полной мере назвать существенными условиями (в том виде, в котором они раскрываются в ст. 432 ГК РФ), поскольку они не детализированы, т. е. не названы в этом правовом акте как «существенные» или «необходимые» условия для характеризуемого договора [7].

Несмотря на многоаспектный характер оказания услуг и их значимость в современном гражданском обороте, сущность этого понятия как объекта гражданских прав не раскрывается в ГК РФ и в других актах гражданского законодательства. Очевидно, законодатель пошел по пути дифференциации каждого вида услуг, определяя их соответствующие понятия в специальных главах кодекса или в специальных законах (иных правовых актах), сущность которых раскрывается, как правило, в системе определенной договорной конструкции.

При определении понятия «оказание услуг как объект гражданских прав» целесообразно использовать метод цивилистического толкования, базирующийся на лексическом и юридическом анализе соответствующих терминов и последующем синтезе полученных результатов [1. С. 98].

Таким образом, прежде всего необходимо дать словесное и юридическое толкование терминам «оказание» и «услуга».

В лексическом контексте глагол «оказать» применяется в сочетании с существительным и означает «действия по назначению данного существительного»

[4. С. 447]. В свою очередь, под услугой понимается «... польза, помощь другому» лицу [4. С. 837]. Таким образом, в словесном выражении оказание услуг – это действия, совершаемые с целью пользы, помощи другому лицу.

В юридической литературе, как правило, рассматривается не термин «оказание услуг», а только его составная часть «услуга». Установим правовую сущность термина «услуга» применительно к системе гражданского законодательства, понимаемого в «узком» и «широком» смысле слова. В первом случае обратим внимание на ГК РФ и принятые в соответствии с ним федеральные законы (п. 2 ст. 3 ГК РФ), во втором – на иные правовые акты (указы Президента РФ и постановления Правительства РФ), а также на акты федеральных органов исполнительной власти (п. 3–7 ст. 3 ГК РФ). Кроме того, следует иметь в виду и подходы судебных органов к толкованию изучаемого термина.

ГК РФ не дает легального универсального определения этого понятия. Однако его сущность можно установить, исходя из анализа общих и специальных положений ГК РФ о договорном регулировании оказания услуг. Так, в ст. 779 сущность договора возмездного оказания услуг заключается в совершении исполнителем по заданию заказчика определенных действий или в осуществлении определенной деятельности, которые заказчик обязуется оплатить.

В названной статье Кодекса стороны договора именуются заказчиком и исполнителем. Однако по отношению к термину «услуга» (в контексте совершаемых действий) для одного лица действия направлены на «получение услуги», а для другого – на то, чтобы «дать услугу».

В Федеральном законе от 07.02.1992 № 2300-1 «О защите прав потребителей», получившем широкое распространение в практике гражданского оборота, термин «оказание (оказать) услуг» упоминается в основном вместе с другими объектами гражданских прав («работы», «товар») и не детализируется в изучаемом аспекте. В то же время, рассматривая отдельные статьи закона (ст. 4, 7 и др.), можно выявить ряд свойств, присущих оказанию услуг, в частности: договорный характер, соответствие «обычно предъявляемым требованиям», «пригодность для целей, для которых услуга обычно используется», «безопасность для жизни, здоровья потребителя, окружающей среды», оказание услуги лицом, имеющим правовое положение «исполнитель» и др.

Среди иных правовых актов прежде всего следует выделить правила оказания различного рода услуг, утверждаемых соответствующими актами Правительства РФ. В подтверждение этому можно привести нормы Постановления Правительства Российской Федерации от 15.09.2020 № 1441 о предоставлении «образовательных услуг» только их исполнителем, а также по заданию и за счет средств заказчика услуг на основании соответствующего договора [5].

Позиция судебных органов в определении понятия «оказание услуг» заключается в соответствующем толковании предметного состава определенных договорных конструкций. Так, предметом договоров оказания услуг является совокупность непосредственных действий или определенного вида деятельности, совершаемых услугодателем [5]. Как отмечается в пункте 3 Постановления Пленума Верховного Суда Российской Федерации от 25 декабря 2018 года № 49 «О некоторых вопросах

применения общих положений Гражданского кодекса Российской Федерации о заключении и толковании договора», в соответствии с пунктами 1 и 2 статьи 429.4 ГК РФ плата по абонентскому договору может взиматься в форме фиксированного платежа, в том числе периодического, или в ином виде (например, товарная поставка), которая не зависит от объема предоставляемого исполнителем выполнения. Отсутствие выполнения абонентом действий по получению выполнения (например, направление запроса исполнителю, невостребование предложенных возможностей непосредственного взаимодействия и т. д.), или получение выполнения в меньшем объеме, чем предусмотрено абонентским договором, как правило, не освобождает абонента от обязанности выплачивать суммы по абонентскому договору. Однако закон или договор могут предусматривать иное, а также это может вытекать из существа законодательного регулирования соответствующего обязательства (пункт 2 ст. 429.4 ГК РФ). Таким образом, согласно ст. 421, 779 ГК РФ договор на абонентское обслуживание не исключает возможность взимания оплаты не только за конкретные услуги, но и за саму возможность обратиться за услугой.

Таким образом, суд в совокупности с отсутствием подписанного двумя сторонами акта оказанных услуг, пришел к выводу о том, что требования истца удовлетворению не подлежат [6]. Апелляционная инстанция оставила решение в силе.

Таким образом, в юридическом смысле «оказание услуг» представляет собой «действия (осуществление деятельности) исполнителя (услугодателя), совершаемые по заданию и с пользой (ценностью) для заказчика (услугополучателя), основанные на договоре».

Выявим специфические признаки детективных услуг и дадим характеристику каждому из них.

1) ограниченный характер. Данный признак означает, во-первых, что оказание услуг происходит только частным детективом или детективной организацией. Во-вторых, детективные услуги оказываются только клиентам-заказчикам, при этом находясь в рамках договорных ограничений, в рамках чего должны быть указаны как содержание и объем предлагаемых услуг, так и предварительные суммы денежных затрат и гонорар за их предоставление [8];

2) информационно-собирательный, поисково-разыскной характер действий услугодателя (исполнителя услуг). Данный признак говорит сам за себя, так как детектив в целях осуществления своих обязанностей по договору собирает информацию и ведет поисковую (поиск имущества физических лиц и организаций) и разыскную (розыск людей) в соответствии с заданием услугополучателя (заказчика-клиента);

3) частноправовой характер. Специфика частноправовой сути услуг, отражающая публично-правовой характер, заключается (в соответствии с п.7 ст. 3 Закона о сыске) в обязанности детектива в письменной форме уведомить лицо, проводящее дознание, следователя или суд, занимающиеся уголовным делом, о проведении договорных мероприятий по сбору информации по уголовным делам в течение суток со дня заключения такого договора с клиентом на сбор подобной информации [9]. Также в рамках статьи 7 данного закона детектив обязан сообщать о фактах планируемых, совершаемых или совершенных преступлений.

Также услуги, в рамках которых происходит поиск информации по уголовным делам и розыск должников в рамках исполнительного производства, затрагивают общественные сферы права (уголовное и исполнительное). Тем не менее направленность услуг на получение информации о гражданах для оформления с ними трудовых правоотношений подтверждает проникновение в сферу частноправовых областей права;

4) потребительский или предпринимательский характер. Сосредоточенность на достижении полезного эффекта от услуг со стороны клиента как потребителя или предпринимателя проявляется в том, что клиент получает необходимый материальный результат в виде информации или имущества за вознаграждение. Исходя из целей предоставления услуг, они могут иметь как предпринимательский, так и потребительский характер. При этом, согласно гражданскому законодательству, извлечение прибыли от оказания детективных услуг подтверждает предпринимательскую направленность таких услуг (ст. 2 ГК РФ). Тот же факт, что полезный эффект от результата сыскных услуг достигается в личных, семейных и иных целях, подтверждает потребительские свойства названных услуг, исключая при этом предпринимательские качества [10];

5) «поименованный» характер услуг выражается в закреплении их в качестве закрытого перечня в ст. 9 Закона о сыске.

На основе проведенного анализа понятий «предмет договора» и «детективная услуга» видится возможным синтезировать их и сформулировать понятие предмета договора оказания детективных услуг как процесс оказания детективных (сыскных) услуг, осуществляемый в форме совершения частным детективом или детективной организацией (услугодатель) по заданию заказчика определенных соглашением сторон действий, направленных на получение заказчиком полезного эффекта, не обладающего материальным результатом и неотделимых от исполнителя.

Совершенствование гражданских правоотношений и активное развитие ЧДД, сочетающей в себе предпринимательские, потребительские, профессиональные свойства, наталкивают на поиск новых моделей осуществления и защиты гражданских прав, что приводит к повышенному вниманию при выборе заказчиком тех или иных видов сыскных услуг. Поэтому становится очевидной необходимость классифицировать исследуемые услуги, так как именно они выступают фундаментом при выборе основания совершения исполнителем детективных услуг необходимого набора действий, при котором услуги обретают свои полезные свойства для всех участников обозначенных гражданских правоотношений.

Список литературы

1. Васьковский Е. В. Цивилистическая методология. Учение о толковании и применении гражданских законов. М.: Центр ЮрИнфоР, 2002.

2. Закон РФ от 11 марта 1992 г. № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации» // Российская газета. 1992. № 100.

3. Информационное письмо Президиума ВАС РФ от 29.09.1999 № 48 «О некоторых вопросах судебной практики, возникающих при рассмотрении споров, связанных с договорами на оказание правовых услуг» // Вестник ВАС РФ. 1999. № 11.

4. Ожегов С. И. Словарь русского языка: 70000 слов / под ред. Н. Ю. Шведовой. М.: Рус. яз., 1989.

5. Постановление Правительства Российской Федерации от 15 сентября 2020 г. № 1441 «Об утверждении Правил оказания платных образовательных услуг» // СЗ РФ. 2020. № 39. Ст. 6035.

6. Решение Арбитражного суда Красноярского края от 11 августа 2020 г. по делу № А32-42597/2019 // СПС «КонсультантПлюс».

7. Шаронов С. А. Сходства, различия и проблемы договорного регулирования частной охранной и частной детективной деятельности на современном этапе развития гражданского оборота // Вестник Московского университета МВД России. 2022. № 5. С. 300.

8. Наумова Е. В. Организационно правовые основы регулирования частной охранной деятельности в Российской Федерации // Казанская наука. 2011. № 1. С. 265-267.

9. Асланян Э. С. Правозащитная деятельность частных охранных организаций и детективных (сыскных) агентств в системе институтов гражданского общества // Образование и право. 2016. № 3. С 161-169.

10. Шаронов С. А. Понятие, правовая природа и классификация оказания охранных услуг как объекта гражданских прав в контексте осуществления предпринимательской охранной деятельности // Вестник Санкт-Петербургского университета МВД России. 2018. № 2(78). С. 126-130.

Ю. В. Ершова,
кандидат юридических наук, доцент,
Московский государственный юридический университет
имени О. Е. Кутафина (МГЮА),
Оренбургский институт (филиал)

О НАЧАЛЕ ПРАВОВОГО РЕГУЛИРОВАНИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Аннотация. В статье анализируется новейший этап развития правового регулирования экономики Российской Федерации, выражающийся в необходимости формирования нормативной базы именно цифровой экономики. Исследовано отношение государственных органов к данному процессу. Выявлены основные нормативные правовые акты, составляющие базу правового регулирования цифровой экономики, а также особенности их содержания. Проанализированы сложности формирования законодательства, связанные с необходимостью регулирования быстро изменяющихся технологий.

Ключевые слова: цифровая экономика, цифровые технологии, цифровое правовое регулирование, цифровое правотворчество, правоприменение, эффективность законодательства, информационные отношения, цифровое право, информационные технологии, цифровое правоотношение, стратегия развития, объекты цифровых прав

ABOUT THE BEGINNING OF LEGAL REGULATION OF THE DIGITAL ECONOMY

Abstract. The article analyzes the latest stage in the development of legal regulation of the economy of the Russian Federation, expressed in the need to form a regulatory framework specifically for the digital economy. The attitude of government agencies to this process has been studied. The main regulatory legal acts that form the basis of legal regulation of the digital economy, as well as the features of their content, have been identified. The difficulties of forming legislation related to the need to regulate rapidly changing technologies are analyzed.

Keywords: digital economy, digital technologies, digital legal regulation, digital lawmaking, law enforcement, effectiveness of legislation, information relations, digital law, information technology, digital legal relations, development strategy, objects of digital rights

Активное внедрение цифровых, информационно-телекоммуникационных, электронных, интеллектуальных технологий [19, 23], в том числе технологий обработки данных, их передачи, документооборота, фиксации результатов имущественного оборота, в различные виды экономической деятельности, автоматизация промышленности и сферы осуществления работ и услуг обуславливают необходимость трансформации экономики в цифровой формат.

Ученые [17] отмечают уже достаточно длительное существование соответствующей терминологии и то, что первым значимым упоминанием термина «цифровая экономика» принято считать монографию 1994 г. Дона Тапскотта «Электронно-цифровое общество» [11. С. 212].

Концепция цифровой экономики, основанной на переходе в экономической, хозяйственной деятельности от «бумаги» к «файлу» имеет в качестве плюсов оперативность контента, отсутствие бумажного документооборота, значительное уменьшение потребностей в сырье.

Авторами выделяются несколько этапов становления цифровой экономики:

1. 1990–2005 гг. – зарождение, формирование цифровых продуктов и электронных услуг.

2. 2005–2010 гг. – их значительное увеличение.

3. 2010–2015 гг. – проникновение цифровых технологий в традиционный бизнес.

4. 2015–2020 гг. – хаотичное перестраивание бизнес-процессов и трансформация бизнес-моделей [20. С. 19] под новые, хаотично и быстро возникающие требования государства по цифровизации процессов.

Правоведы в настоящее время стоят перед необходимостью обеспечить механизм правового регулирования цифровой экономики. Причем это должны быть такие средства и способы регулирования, которые отвечали бы скорости изменений, с одной стороны, а с другой – давали субъектам права, субъектам гражданского оборота необходимые гарантии реализации их прав. Как указывает С. А. Дятлов, «правоотношения лиц в Интернете должны существовать в особом правовом поле, адекватно учитывающем специфику сетевого интернет-пространства и имеющем свои особенные нормативно-регламентирующие принципы» [14. С. 87].

С позиции теории права нормативное (правовое, законодательное) обеспечение цифровой экономики представляет собой совокупность юридических мер, средств и способов, направленных на установление *регулирования организации и функционирования совокупности общественных отношений, складывающихся в гражданском обороте и публичной сфере в цифровой среде с применением цифровых технологий.*

До настоящего времени отсутствует единая дефиниция цифровой экономики. При этом в публикациях мы видим множество терминов, близких к рассматриваемому либо определяющих его подвид, в частности, «интернет-экономика», «электронная экономика», «экономика приложений», «программируемая экономика», «креативная экономика» и т. д.

Всемирным банком цифровая экономика трактуется как «система экономических, социальных и культурных отношений, основанных на использовании цифровых информационно-коммуникационных технологий» [24].

Оксфордский словарь определяет ее как «экономику, которая главным образом функционирует за счет цифровых технологий, особенно электронных транзакций, осуществляемых с использованием Интернета» [12. С. 310].

Укажем на авторов, дающих собственные определения, для возможного ознакомления читателями. Это, в частности, В. А. Вайпан [13. С. 7], Н. А. Стефанова и Т. Э. Рахманова [25. С. 301], А. И. Мозговой [22. С. 37], Л. В. Лапидус [20. С. 21] и многие другие. Некоторые из аспектов регулирования «цифры» рассматривались и автором настоящего исследования [16. С. 417–422].

Значимым является то, что государственные структуры обращают особое внимание на необходимость создания правового поля для цифровой экономики.

Впервые на необходимости формирования системных подходов к цифровой экономике было сказано Президентом России В. В. Путиным в 2016 г. в Послании Федеральному Собранию. *Определение цифровой экономики сформулировано в У*казе Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» [6], согласно которому «цифровая экономика – хозяйственная деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг».

На состоявшемся 5 июля 2017 г. заседании Совета при Президенте РФ по стратегическому развитию В. В. Путин отметил, что «цифровая экономика – это новая основа для развития системы государственного управления, экономики, бизнеса, социальной сферы, всего общества. Ее формирование – вопрос национальной безопасности и независимости России, конкурентности отечественных компаний, позиций страны на мировой арене на долгосрочную перспективу».

Итогом данного посыла стала программа «Цифровая экономика Российской Федерации» [8], которая содержит определение ее как «хозяйственной деятельности, ключевым фактором производства в которой являются данные в цифровой форме, и способствует формированию информационного пространства с учетом потребностей граждан и общества в получении качественных и достоверных сведений, развитию информационной инфраструктуры Российской Федерации, созданию и применению российских информационно-телекоммуникационных технологий, а также формированию новой технологической основы для социальной и экономической сферы».

Авторы исследуют данные определения с позиции правотворчества и его уровня [26. С. 28; 18. С. 41; 21. С. 12].

Национальная программа «Цифровая экономика Российской Федерации» [9], разработанная в том числе Советом при Президенте Российской Федерации по стратегическому развитию и национальным проектам, указывает на направления ее развития, среди которых базовым является нормативное регулирование цифровой среды, основной задачей которого является создание системы правового регулирования цифровой экономики, основанной на гибком подходе к каждой сфере, а также внедрение гражданского оборота на базе цифровых технологий [10]. Реализация программы планируется поэтапно в период до 2024 года.

Сложившаяся в настоящее время система нормативных правовых актов, регулирующих цифровую экономику, относится, главным образом, к электронной торговле и электронному документообороту. Это в том числе Федеральный закон от 18 марта 2019 г. № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» [2], Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи» [3], Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [4], Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» [5], Постановление Правительства РФ от 27 сентября 2007 г. № 612 «Правила продажи товаров дистанционным способом» [7], некоторые другие.

В ГК РФ законом от 18 марта 2019 г. было введено понятие «цифровые права», под которыми понимаются обязательственные или иные права, оборот которых возможен только в информационной системе.

Закон № 149-ФЗ закрепляет основные определения «информационной системы», «информационных технологий», «информационно-телекоммуникационной сети», «сайта в сети Интернет» и других терминов, имеющих максимальное значение в правовом регулировании цифровой экономики.

Закон № 152-ФЗ регламентирует порядок обработки персональных данных с использованием автоматизированных баз данных.

Перед правоведами и законодателем поставлена задача, которая сопряжена с определенными сложностями. Основными из них, на наш взгляд, являются:

Опережающее, стремительное развитие информационных технологий. Нормативное описание «цифры» отстает от ее развития во времени.

Неопределенность состава и границ образуемых правовых институтов. Мы говорили о неоднозначном отношении к регулированию, например, криптовалюты [16. С. 417–422], аккаунтов, цифровых счетов [15. С. 84–90]. Законодатель пока не понимает то, что именно необходимо регулировать, и подбирает приемы и способы законодательной техники к объектам цифровых отношений.

Стандартное регулирование направлено на установление прообраза надлежащих отношений между людьми. В цифровой же экономике следует регулировать качество технологических процессов при участии в них людей.

С учетом названных особенностей быстрая регламентация цифровизации осуществляется на основе документов стратегического планирования – национальных и государственных программ и стратегий, которые, помимо скорости принятия, имеют и еще один плюс – они предусматривают мероприятия, направленные на стимулирование внедрения цифровых технологий в экономику и тем самым способствуют ее расширению, проникновению во множество сфер реальной экономики.

Указанные выше проблемы нивелируются отчасти Федеральным законом от 31 июля 2020 г. № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» [1]. Закон № 258-ФЗ определяет посредством открытого перечня основные направления, в которых могут устанавливаться экспериментальные правовые режимы в сфере цифровых инноваций. Это в том числе финансовый рынок, медицина, сельское хозяйство, дистанционная продажа, строительство, предоставление государственных и муниципальных услуг и осуществление государственного контроля (надзора) и муниципального контроля; промышленность.

Можно образно сказать, что государство посредством установления экспериментальных правовых режимов «подбирает» должное регулирование.

Принятие Закона № 258-ФЗ многие ученые и правоприменители оценивают положительно, поскольку он регулирует технологии, которые уже используются на практике.

Таким образом, в настоящее время ученые-правоведы и законодатель находятся на весьма интересном этапе, когда развитие реальной экономики в направлении цифровизации понуждает обращаться к нестандартным, специфичным и оттого весьма интересным приемам и способам регулирования общественных отношений.

Список литературы

1. Федеральный закон от 31.07.2020 № 258-ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» // Собрание законодательства РФ. 2020. № 31 (часть I). Ст. 5017.

2. Федеральный закон от 18.03.2019 № 34-ФЗ «О внесении изменений в части первую, вторую и статью 1124 части третьей Гражданского кодекса Российской Федерации» // Собрание законодательства РФ. 2019. № 12. Ст. 1224.

3. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи» // Собрание законодательства РФ. 2011. № 15. Ст. 2036.

4. Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3448.

5. Федеральный закон от 27.06.2006 № 152-ФЗ «О персональных данных» (с изм. и доп. от 24 апреля 2020 г. № 123-ФЗ) // Собрание законодательства РФ. 2006. № 31 (ч. 1). Ст. 3451.

6. Указ Президента Российской Федерации от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

7. Постановление Правительства Российской Федерации от 27.09.2007 № 612 «Об утверждении Правил продажи товаров дистанционным способом» // Собрание законодательства РФ. 2007. № 41. Ст. 4894.

8. Распоряжение Правительства Российской Федерации от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации» (утратило силу) // Собрание законодательства РФ. 2017. № 32. Ст. 5138

9. Протокол от 24 декабря 2018 г. № 16 Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам Национальная программа «Цифровая экономика Российской Федерации». URL: https://home.garant.ru

10. Паспорт федерального проекта «Цифровые технологии» (утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности. URL: https://digital.gov.ru/ru/

11. Tapscott D. The Digital Economy Anniversary Edition: Rethinking Promise and Peril In the Age of Networked Intelligence. N.Y.: McGraw-Hill, 2014.

12. Большой оксфордский толковый словарь английского языка = Oxford school dictionary : 45000 слов и выражений / под ред. А. Делаханти и Ф. Макдональда. М.: АСТ ; Oxford : Астрель, 2005. 807 с.

13. Вайпан В. А. Основы правового регулирования цифровой экономики // Право и экономика. 2017. № 11(357). С. 5-18.

14. Дятлов С. А. Цифровая экономика: новые методологические проблемы исследования // Современные технологии: актуальные вопросы, достижения и инновации: сборник статей IX Международной научно-практической конференции. Пенза, 27 сентября 2017 года / под общей ред. Г. Ю. Гуляева. Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2017. С. 84-88.

15. Ершова Ю. В., Конева А. В. Проблемы правового регулирования наследования объектов цифровых прав // Труды Оренбургского института (филиала) Московской государственной юридической академии. 2023. № 2(56). С. 84-90.

16. Ершова Ю. В., Лысенко В. К. Криптовалюта как объект корпоративного права: тенденции развития законодательства // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции. В 6 т., Казань, 23 сентября 2022 года. Казань: Познание, 2022. С. 417-422.

17. Ищенко М. В. Цифровая экономика в теоретическом аспекте // Вестник СИБИТа. 2020. № 4(36).

18. Ковалев А. Е. Перспектива формирования единого пространства учетной информации в складывающейся цифровой экономике // Аудитор. 2019. Т. 5, № 3. С. 41-50.

19. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7-32. EDN LCCOJJ.

20. Лапидус Л. В. Что такое цифровая экономика и Индустрия 4.0? Принципы трансформации и перспективы для бизнеса // Перспективы развития электронного бизнеса и электронной коммерции: материалы IV Межфакультетской научно-практической конференции молодых ученых. М., 2018. С. 19-21.

21. Маракулин М. В. Понятие «цифровой экономики» в государственной программе «цифровая экономика Российской Федерации» // Пермский край: новые вызовы, новое время: материалы IV Пермского экономического конгресса, Пермь, 8 февр. 2018 г. Пермь: Пермский государственный национальный исследов. ун-т, 2018. С. 339-344.

22. Мозговой А. И. Повышение эффективности управления за счет цифровизации экономики // Вестник евразийской науки. 2018. Т. 10, № 5. С. 37-54.

23. Резаев А. В., Трегубова Н. Д. Возможность и необходимость человеко-ориентированного искусственного интеллекта в юридической теории и практике // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 564-580. EDN SADRZW.

24. Семинар Всемирного банка. 20 декабря 2016 г. URL: https://www.youtube.com/watch?v=-QLI_b9gnbM

25. Стефанова Н. А., Рахманова Т. Э. Оценка эффективности цифровой экономики // Карельский научный журнал. 2017. № 4 (21). С. 301-303.

26. Якутин Ю. В. Российская экономика: стратегия цифровой трансформации: к конструктивной критике правительственной программы «Цифровая экономика Российской Федерации» // Менеджмент и бизнес-администрирование. 2017. № 4. С. 27-52.

Е. А. Кириллова,
кандидат юридических наук, доцент,
Юго-Западный государственный университет
Т. Э. Зульфугарзаде,
кандидат юридических наук, доцент,
Российский экономический университет
имени Г. В. Плеханова

ПРОБЛЕМЫ АВТОРСТВА ПРОИЗВЕДЕНИЙ, СОЗДАННЫХ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Аннотация. В статье рассматриваются проблемы авторства произведений, созданных искусственным интеллектом. Стремительное развитие технологий, нейросетей и искусственного интеллекта породило множество вопросов, одним из которых является определение авторства произведений, полностью созданных искусственным интеллектом. Предметом анализа становятся различные подходы в сфере регулирования интеллектуальной собственности с учетом роли искусственного интеллекта. Применяются обще- и частнонаучные методы: анализа, синтеза, аналогии, формально-юридический, сравнительно-правовой, толкования правовых норм и др. Выделены три основных подхода в охране прав на результаты интеллектуальной деятельности, созданные искусственным интеллектом. Сделан вывод, что введение специального права для регулирования правоотношений с участием искусственного интеллекта позволит защитить права людей, которые причастны к созданию творческих произведений, и обеспечат охрану результатов интеллектуальной деятельности. В дальнейшем научном осмыслении нуждаются вопросы охраны результатов интеллектуальной деятельности, созданной искусственным интеллектом, так как существует неопределенность с принадлежностью авторских прав на созданные произведения.

Ключевые слова: искусственный интеллект, интеллектуальная собственность, имущественные права, защита прав, правосубъектность, творческий продукт, технологические решения, цифровизация, цифровая среда, нейросеть, авторские права, объект права, субъект права, обязанности, правопреемство

PROBLEMS OF AUTHORSHIP OF WORKS CREATED BY ARTIFICIAL INTELLIGENCE

Abstract. The article discusses the problems of authorship of works created by artificial intelligence. The rapid development of technologies, neural networks and artificial intelligence has given rise to many questions, one of which is the determination of the authorship of works completely created by artificial intelligence. Methods. The subject of the analysis is various approaches in the field of intellectual property regulation, taking into account the role of artificial intelligence. General and private scientific methods are used – analysis, synthesis, analogy, formal legal, comparative legal, interpretation of legal norms, etc. Results. There are three main approaches to the protection of intellectual property rights created by artificial intelligence. It is concluded

that the introduction of a special law to regulate legal relations involving artificial intelligence will protect the rights of people who are involved in the creation of creative works and ensure the protection of the results of intellectual activity. Discussion. The issues of protection of the results of intellectual activity created by artificial intelligence need further scientific understanding, since there is uncertainty about the ownership of copyrights to the created works.

Keywords: artificial intelligence, intellectual property, property rights, protection of rights, legal personality, creative product, technological solutions, digitalization, digital environment, neural network, copyright, object of law, subject of law, obligations, succession

Введение. В 2019 году была принята «Национальная стратегия развития искусственного интеллекта на период до 2030 года» в которой отмечалось, что происходит ускоренное внедрение технологических решений, разработанных на основе искусственного интеллекта во всех сферах экономических, социальных, общественных отношений. На вопросы по телефону отвечают голосовые помощники, заказы оформляют боты, они же ведут переписку с клиентами, использование искусственного интеллекта и нейросетей применяется на государственном уровне, примеры можно приводить бесконечно. Многие разработки невозможно создать без использования программ, более того, искусственный интеллект достиг такого уровня, когда он успешно конкурирует с человеком. Например, широко освещался цифровой скандал, когда студент РГГУ написал дипломную работу с помощью ChatGPT, который представляет собой программу способную создавать интернет-сайты, писать статьи и песни, при этом уникальность созданной работы составила 82 %, а время, затраченное на создание диплома, составило всего 23 часа [7]. В 2019 году в патентные ведомства ЕС и США учеными были поданы заявки на выдачу патентов на изобретения, где в качестве автора изобретения был указан Dabus – искусственный интеллект [3]. Искусственный интеллект широко и активно используется в различных сферах, поэтому возникает необходимость правового регулирования правоотношений, связанных с роботовызовами. Развитие автономности искусственного интеллекта требует пересмотра правовых режимов, а также подотраслей, институтов, таких как режим правовой ответственности искусственного интеллекта, налогообложение любой деятельности с использованием искусственного интеллекта, электронная коммерция с участием ботов, электронных личностей, регулирование прав интеллектуальной собственности, когда произведения создаются с помощью искусственного интеллекта или полностью искусственным интеллектом.

Одна из проблем связана с определением правосубъектности искусственного интеллекта в области создания творческих произведений. Данная проблема представляет теоретический и практический интерес и требует комплексного анализа. Основная цель исследования – рассмотреть основные подходы регулирования правоотношений с участием искусственного интеллекта в сфере создания интеллектуальных продуктов.

Основная часть. Технологии искусственного интеллекта развиваются стремительно и вопросы, возникающие в сфере его применения требуют реагирования на законодательном уровне. Одной из проблем является квалификация созданных искусственным интеллектом результатов интеллектуальной деятельности. На практике сложно однозначно ответить, кто является их автором: пользователь программы, создатель программы или сама программа, то есть искусственный интеллект, который не является субъектом правоотношений. Также возникают вопросы охраны результатов интеллектуальной деятельности, созданной искусственным интеллектом, так как существует неопределенность с принадлежностью авторских прав на созданные произведения. Поэтому необходимо определить границы правосубъектности искусственного интеллекта и правовой статус результатов интеллектуальной деятельности, созданной искусственным интеллектом. Вопросы охраны произведений, созданных искусственным интеллектом или с его значительным участием, активно обсуждаются, но решений не найдено, не сформирована модель регулирования в данной сфере и даже не создан понятийный аппарат. Определение дефиниции «искусственный интеллект» вызывает дискуссии среди экспертов [6], впервые данное определение было закреплено в Указе Президента РФ от 1010.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», впоследствии оно было использовано в Федеральном законе от 24 апреля 2020 г. № 123-ФЗ «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации – городе федерального значения Москве и внесении изменений в статьи 6 и 10 Федерального закона «О персональных данных» (далее Закон №123-ФЗ). В соответствии с Законом № 123-ФЗ искусственный интеллект – это комплекс технологических решений, который позволяет имитировать когнитивные функции человека и получать результаты сопоставимые с результатами интеллектуальной деятельности человека. Авторские произведения, созданные искусственным интеллектом, как и любые произведения, нуждаются в правовой защите, однако на практике это представляет сложную дилемму. Неспособность защитить произведение, созданное искусственным интеллектом, может оставить интерпретаторов таких произведений без прав, так как защита, предоставляемая смежными правами, предполагает наличие авторских прав на интерпретируемое произведение.

В охране прав на результаты интеллектуальной деятельности, созданные искусственным интеллектом, можно выделить три основных подхода:

– произведения, созданные искусственным интеллектом, не должны охраняться;

– произведения, созданные искусственным интеллектом, должны охраняться авторским правом;

– произведения, созданные искусственным интеллектом, должны охраняться смежным правом.

Исследователи, предлагающие отменить охрану прав на произведения, созданные искусственным интеллектом, аргументируют данную позицию тем, что в данном случае субъекты и объекты в создавшихся правоотношениях столь специфич-

ны, что невозможно обеспечить защиту авторских прав, учитывая правовой статус создателя произведения [8. С. 819–844]. В таких случаях можно было бы распространить на объекты, созданные искусственным интеллектом, режим общественного достояния, но возникнут проблемы авторства, возможности интерпретации произведения и другие. Поэтому данный подход вызывает справедливые сомнения.

Точка зрения, что произведения, созданные искусственным интеллектом, должны охраняться авторским правом, практически не находит поддержки среди исследователей, справедливо выдвигаются аргументы, что искусственный интеллект не правосубъектен, и поэтому произведения, созданные им, не могут подлежать защите в рамках авторского права, однако предлагается защищать личные неимущественные права автора программы, которая и создает результат интеллектуальной деятельности [4. С. 69]. Подход, в рамках которого произведения, созданные искусственным интеллектом, должны охраняться смежным правом, наиболее востребован, так как позволяет обеспечить охрану прав на произведение с учетом специфических особенностей возникающих правоотношений и особого статуса созданных произведений. Достаточно редко высказывалось мнение, что авторские произведения, созданные искусственным интеллектом, должны охраняться в рамках вещного права, но данная позиция была подвергнута критике и не нашла поддержки в цивилистике [2. С. 7–18]. Возникают вопросы о том, кто является субъектом права при создании произведения искусственным интеллектом, и здесь мнения экспертов разделились, например, высказывалось радикальное мнение, что права на произведения должны принадлежать искусственному интеллекту [1. С. 157–170], однако большинство экспертов предлагают закрепить права на созданное произведение за разработчиками искусственного интеллекта [9. С. 193–199] или за организаторами процесса использования искусственного интеллекта [5. С. 76–77]. Искусственный интеллект является инструментом, с помощью которого создаются интеллектуальные продукты, права на которые должны быть признаны за программистами или лицами, которые используют программу для создания творческих произведений [10].

В законодательстве стран Западной Европы и США регламентирован подход, при котором искусственный интеллект признается объектом права, поэтому все права на произведения, созданные искусственным интеллектом даже без участия человека, закрепляются за физическими лицами [11. P. 763–767]. Но не все страны придерживаются такого подхода, так, в Южной Корее предлагается кардинально изменить законодательство и признать права электронных лиц, то есть искусственного интеллекта, в таких условиях вопросы правовой охраны произведений, созданных искусственным интеллектом, будут решены по аналогии с защитой произведений, созданных физическими лицами, таким образом, искусственный интеллект будет уравнен в правах с людьми [12]. Введение подобной новеллы означает пересмотр существующих принципов регулирования в сфере интеллектуальной собственности, при этом с введением нового субъекта права происходят концептуальные изменения в доктрине гражданского права. Такие кардинальные изменения должны осуществляться только при наличии серьезных правовых, социальных, экономических оснований [13. С. 1– 22].

Заключение. Минимальным нововведением в российском законодательстве может стать разграничение результатов интеллектуальной деятельности на созданные искусственным интеллектом и на созданные с использованием искусственного интеллекта. Когда произведения создаются с использованием искусственного интеллекта, авторские права принадлежат физическому лицу, в случае когда произведение целиком и полностью создано искусственным интеллектом возникает необходимость специального правового регулирования. Исключение творческого труда человека из процесса создания произведения дает основания для специального правового регулирования в ситуациях, когда интеллектуальный объект полностью создан искусственным интеллектом. Возможно, созданные таким образом произведения будут частично исключены из сферы охраны, что не означает отсутствие защиты прав разработчика искусственного интеллекта, который создал программу, способную создавать творческие произведения. Лицу, организовавшему создание творческого произведения искусственным интеллектом, должна быть обеспечена защита прав по аналогии с защитой прав изготовителя фонограммы или изготовителя базы данных, то есть право авторства, право на неприкосновенность произведения, право на обнародование, отзыв. Введение специального права для регулирования правоотношений с участием искусственного интеллекта позволит защитить права людей, которые причастны к созданию творческих произведений и позволят обеспечить охрану результатов интеллектуальной деятельности.

В случаях, когда творческое произведение создается с помощью искусственного интеллекта, правоотношения могут регулироваться традиционным образом, при этом искусственный интеллект рассматривается как объект права, с помощью которого человек создает интеллектуальные продукты.

Такой дифференцированный подход позволит разграничить сферы правового регулирования в сфере защиты интеллектуальной собственности, созданной искусственным интеллектом или с участием искусственного интеллекта.

Список литературы

1. Архипов В. В., Наумов В. Б. О некоторых вопросах теоретических оснований развития законодательства о робототехнике: аспекты воли и правосубъектности // Закон. 2017. № 5. С. 157-170.

2. Гурко А. Искусственный интеллект и авторское право: взгляд в будущее // ИС. Авторское право и смежные права. 2017. № 12. С. 7-18.

3. Калиничева М. О некоторых вопросах правовой охраны изобретений, созданных искусственным интеллектом // Закон. Электронный ресурс. URL: https://zakon.ru

4. Камалова Г. Г., Наумов М. В., Незнамов А. В. и др. Модели правового регулирования создания, использования и распространения роботов и систем с искусственным интеллектом. СПб., 2019.

5. Нагродская В. Б. Новые технологии (блокчейн/искусственный интеллект) на службе права: научно-методическое пособие / под ред. Л. А. Новоселовой. М.: Проспект, 2019.

6. Незнамов А. В. Правовые аспекты реализации национальной Стратегии развития искусственного интеллекта до 2030 года // Вестник Университета имени О. Е. Кутафина. 2019. № 12(64).

7. Нейросеть за один вечер написала диплом за российского студента. Преподаватели в шоке – как теперь проверять знания? // Комсомольская правда. URL: https://www.msk.kp.ru

8. Chesterman S. Artificial intelligence and the limits of legal personality // International & Comparative Law Quarterly. 2020. № 69(4). Pp. 819-844.

9. Hema K. Protection of artificial intelligence autonomously generated works under the copyright act, 1957-an analytical study // Journal of Intellectual Property Rights (JIPR). 2023. № 28(3). Pp. 193-199.

10. Kerikmäe T., Müürsepp P., Pihl H. M., Hamuľák O., & Kocharyan, H. Legal Person-or Agenthood of Artificial Intelligence Technologies // Acta Baltica Historiae et Philosophiae Scientiarum. 2020. № 8(2).

11. Protection of Works Generated by Machine Learning Software, GRUR International. 2020. Vol. 69, Iss. 7. Pp. 763-767.

12. Talimonchik V. P. The Prospects for the Recognition of the International Legal Personality of Artificial Intelligence. Laws. 2021. № 10(4). Pp. 85-110.

13. Ziemianin K. Civil legal personality of artificial intelligence: Future or utopia? // Internet Policy Review. 2021. № 10(2). Pp. 1-22.

Н. Е. Коваленко,
аспирант,
Алтайский государственный университет

СУБЪЕКТ ПРАВА И ИНФОРМАЦИОННАЯ ЕДИНИЦА

Аннотация. В статье рассматривается соотношение нормативного содержания субъекта права, заложенного еще с возникновением советского государства и права с теоретическими представлениями в юридической доктрине. Современное информационное общество формирует новое представление о государстве и праве, изменяет содержание законодательства. В силу чего и меняется качественное наполнение понятия «субъект права». Целью статьи отмечаются отдельные новые свойства, которые наполняют содержание термина «субъекта права».

Ключевые слова: право, закон, правоотношение, субъект права, лица, правовое регулирование, Гражданский кодекс

SUBJECT OF LEGAL AND INFORMATION UNIT

Abstract. The article examines the relationship between the normative content of the subject of law, laid down with the emergence of the Soviet state and law, with

theoretical concepts in legal doctrine. The modern information society forms a new idea of the state and law, changes the content of legislation. Due to this, the qualitative content of the concept "subject of law" changes. The purpose of the article is to highlight certain new properties that fill the content of the term "subject of law".

Keywords: law, law, legal relationship, subject of law, persons, legal regulation, Civil Code

Введение. Одним из первых нормативно-правовых актов, закрепляющим статус субъекта права, стал Гражданский кодекс РСФР 1922 года, учрежденный Постановлением ВЦИК от 11.11.1922 «О введении в действие Гражданского кодекса Р.С.Ф.С.Р.». В названном акте глава 2 посвящена субъекту права (лицам). Как можно заметить, законодатель не разводил данные понятия. Содержание главы посвящено двум видам субъекта: физические лица (напрямую указания нет, подразумеваются граждане) и юридические лица (и их формы).

В последующем с принятием уже Гражданского кодекса РСФСР 1964 года, утвержденного Верховным Советом РСФСР 11.06.1964, ситуация не очень изменилась, субъектами оставались все те же виды, с модернизацией правового статуса и расширением организационных форм юридического лица. Данная традиция остается и на сегодняшний день, никто не ставит под сомнение правильность определения субъекта права как физических и юридических лиц. Однако насколько верен с философско-правовой точки зрения был данный подход, заложенный на истоках формирования советского государства и законодательства?

Основная часть. Отвечая на поставленный вопрос, следует обратиться к трудам философа права Н. Н. Алексеева. Согласно его концепции, существует два вида субъекта права: деятельностный субъект и юридический [3, 4].

Для деятельностного субъекта характерно проявление воли, совершение поступков, такие лица способны к деятельности от природы. Юридический же субъект направлен на защиту определенных ценностей, выявляются самоцели правовой регламентации, по сути, это признанная правом ценность.

Н. Н. Алексеев писал, что «именно носить «право» означает быть деятелем, а также признанной и охраняемой правопорядком ценностью» [1. С. 84]. Отметим, что вопрос субъекта поднимали и другие правоведы, к примеру И. А. Ильин. Для него субъект права – индивидуальность, фундаментальный элемент правовой материи, воплощенный в реальность. Все понимание субъекта у ученого сводится к «персоналистской» характеристике [5. С. 405– 410].

Отдельные исследователи отмечают разумное осмысление обсуждаемых правоведами возможностей наделения систем искусственного интеллекта статусом субъекта права [2].

Заключение. Таким образом, приходим к тому, что категория «субъект права» намного объемнее и сложнее, чем ее традиционно представляют как практики, так и теоретики. Поэтому в настоящее время возникают сложности в правовом регулировании отношений с участием неопределенных субъектов, таких как беспилотные транспортные средства и роботы с технологией искусственного интеллекта высокой степенью автономности, нейросети и т. д. Общественные отношения

подвержены изменению и усложнению, правовая база обязана совершенствоваться для их урегулирования, во избежание возникновения правовых пробелов. Если на это не обращать внимания, то возможно падение уровня правовой культуры государства и общества.

Список литературы

1. Алексеев Н. Н. Основы философии права. СПб.: Лань, 1999. 256 с.

2. Филипова И. А., Коротеев В. Д. Будущее искусственного интеллекта: объект или субъект права? // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 359-386. EDN IMMOAM.

3. Коваленко Н. Е. Особенности концептуального подхода С. С. Алексеева к категории «правоотношение» // Вестник Гуманитарного университета. 2023. № 2(41). С. 73-77.

4. Коваленко Н. Е. Деконструкция постмодернизма. Тенденция субъекта права в информационном обществе // Евразийский юридический журнал. 2023. № 1(176). С. 72-73.

5. Ильин И. А. Свободная индивидуальность. В 10 т. Т. 9-10. М.: Русская книга, 1999. 506 с.

А. В. Колосов,
кандидат юридических наук, доцент,
Иркутский государственный университет

ГОСУДАРСТВЕННО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ КОММЕРЧЕСКИХ ОТНОШЕНИЙ В ИНФОРМАЦИОННОЙ СРЕДЕ И LEX INFORMATICA: ВОПРОСЫ СООТНОШЕНИЯ

Аннотация. В статье анализируются особенности государственно-правового регулирования коммерческих отношений в информационной среде и возможности применения альтернативных правил lex informatica. Современное развитие трансграничной коммерческой деятельности в настоящее время претерпевает серьезные изменения, и существующие модели правового регулирования экономических отношений не отвечают объективной реальности, с которой сталкиваются предприниматели в своей ежедневной практике. Вследствие этого требуется поиск новых механизмов регулирования отношений, которые могли бы гибко подстроиться под нужды бизнес-сообщества. Подобными унифицированными положениями, регламентирующими сферу торговых операций в информационной среде, стал свод правил, который получил название lex informatica. Делается вывод, что современные международные коммерческие отношения в интернет-пространстве следует регулировать как с помощью традиционных способов, которыми обладает государство, так и посредством современных инструментов, основанных на актуальной практике трансграничных экономических отношений.

Ключевые слова: lex informatica, государственно-правовое регулирование, информационные отношения, информационная среда, информация, торговля, предпринимательство, цифровое общество

STATE-LEGAL REGULATION OF COMMERCIAL RELATIONS IN THE INFORMATION ENVIRONMENT AND LEX INFORMATICA: ISSUES OF CORRELATION

Abstract. The article analyzes the features of state-legal regulation of commercial relations in the information environment and the possibility of applying alternative lex informatica rules. The modern development of cross-border commercial activity is currently undergoing serious changes, and the existing models of legal regulation of economic relations do not meet the objective reality that entrepreneurs face in their daily practice. As a result, it is necessary to search for new mechanisms for regulating relations that could flexibly adapt to the needs of the business community. Similar unified provisions regulating the sphere of trade operations in the information environment became a set of rules, which was called lex informatica. It is concluded that modern international commercial relations in the Internet space should be regulated both through traditional methods that the state has, and through modern tools based on the current practice of cross-border economic relations.

Keywords: lex informatica, state-legal regulation, information relations, information environment, information, trade, entrepreneurship, digital society

Современное развитие трансграничной коммерческой деятельности в настоящее время претерпевает серьезные изменения, и существующие модели правового регулирования экономических отношений не отвечают объективной реальности, с которой сталкиваются предприниматели в своей ежедневной практике. Глобализация мира и сферы торговли, активное использование сети Интернет в предпринимательской деятельности значительно ускоряют существующие коммерческие операции, способствуют появлению новых видов отношений и технологических инструментов, позволяющих значительно оптимизировать и увеличить экономические формы сотрудничества как среди широкого круга предпринимателей, так и возможности более тесного межгосударственного сотрудничества.

Однако противоречивая экономическая политика стран, отсутствие согласованности действий государств по регулированию сферы торговли и осложненность подобных отношений иностранным элементом порождает проблемы правового регулирования. Особенно остро это проявляется в регулировании торговых отношений в информационной среде. Это связано с тем, что электронная коммерческая деятельность и использование сети Интернет в предпринимательской сфере представляет собой достаточно новую область, которая находится на стадии активного развития, и существующее правовое регулирование не поспевает за технологическим прогрессом, что порождает сложности в регулировании современных отношений в киберпространстве. Кроме того, современные цифровые технологии и возникающие на базе них отношения коммерческого характера не

могут быть исключительно объектом правового регулирования одного государства, так как их трансграничный характер требует согласованных действий всего мирового сообщества с целью создания стабильных, прогнозируемых и эффективных экономических отношений.

Вследствие этого требуется поиск новых механизмов регулирования отношений, которые могли бы гибко подстроиться под нужды бизнес-сообщества и нивелировать все существующие сложности взаимодействия, обусловленные их трансграничным характером.

Исторически сложилось, что благодаря государственному регулированию устанавливаются правила торговых отношений, но в то же время современные технологические возможности определяют необходимость создания принципиально новых подходов при разработке правил электронной торговли и способов осуществления бизнес-деятельности в интернет-пространстве. Подобными унифицированными положениями, регламентирующими сферу торговых операций в информационной среде, стал свод правил, который получил название lex informatica. Появление подобных правил подтверждает ранее возникшую концепцию фрагментации права [1. С. 144], когда к уже существующим традиционным нормотворческим субъектам и нормам права добавляются альтернативные системы правил, которые также могут создаваться международными организациями, международными коммерческими арбитражами и иными субъектами.

Необходимость создания данных правил обуславливается активным развитием цифровых технологий, распространением коммерческих отношений с использованием сети Интернет и необходимостью создания регуляторов, способных обеспечивать взаимодействие сторон в киберпространстве вне существования национальных границ и действия законов.

В научной литературе возникла дискуссия по поводу коммерциализации Интернета и способов регулирования вновь возникающих коммерческих отношений в киберпространстве. По мнению одних исследователей, требуется единообразное правовое регулирование, которое призвано решить все неопределенности современных отношений [3. С. 3].

Другие же ученые отмечают, что современные компьютерные технологии и возникающие на базе них отношения экономического характера невозможно урегулировать правовыми средствами, и есть необходимость создания особых альтернативных правил [2. С. 411].

Думается, что сравнительно-правовой подход при анализе особенностей государственно-правового регулирования коммерческих отношений в информационной среде и возможностей применения альтернативных правил lex informatica позволит внести ясность, понять достоинства и недостатки существующих доктринальных взглядов, а также разграничить рассматриваемые категории.

Во-первых, основу структуры государственно-правового регулирования составляют законы и иные нормативно-правовые акты, принимаемые государством с целью регулирования коммерческих отношений в информационной сфере. В структуру lex informatica входят основные принципы права, международные акты, создаваемые международными организациями, международные торговые обы-

чаи, типовые соглашения и контракты, решения международных коммерческих арбитражей.

Во-вторых, исходя из особенностей указанной выше структуры регулирования можно выделить следующую особенность – характер закрепляемых правил и норм. Зачастую государственно-правовое регулирование использует жесткие и стандартизированные правила регулирования отношений, в то время как нормы lex informatica имеют гибкость и создают возможности для регулирования коммерческих отношений без учета национальной практики и в обход существующих законов. Правилам lex informatica присущ индивидуальный характер, пластичность, что позволяет избежать многих трудностей в случае использования правовых решений государства.

В-третьих, субъекты, создающие нормы, также различны. В случае государственного регулирования коммерческих отношений в информационной среде субъектами правотворчества выступают органы государственной власти и должностные лица. Субъектный состав lex informatica значительно расширяется, и количество субъектов неуклонно растет. Увеличение субъектного состава объясняется тем, что значительно растет бизнес-сообщество, количество арбитров в международных коммерческих арбитражах, экспертов, которые способствуют процессам стандартизации экономических отношений путем разработки шаблонных договоров и правил, имеющие характер образца для предпринимателей из разных стран и зачастую неизвестны национальному праву.

В-четвертых, отличается и способ создания норм. Государство в рамках своего законодательства устанавливает процедуру принятия нормативно-правовых актов. Зачастую это сложный нормотворческий процесс, сопряженный с определенными стадиями прохождения будущего правового акта. Процедура принятия правил lex informatica отличается меньшим формализмом и большой простотой, когда источники создаются «снизу» заинтересованными субъектами и базируются на достижениях практики экономического оборота.

В-пятых, содержание норм в рамках государственно-правового регулирования основывается на законодательно сформулированных положениях, а в странах англо-саксонского права также на судебных прецедентах. Содержание правил lex informatica предусматривает отказ от применения норм национального и коллизионного права и формируется за счет единообразной и прогнозируемой практики участников коммерческой деятельности в информационной среде.

В-шестых, территориальное распространение правил также различно. При государственно-правовом регулировании коммерческих отношений применение норм осуществляется в рамках границ конкретного государства. Правила lex informatica автономны и не зависят от территориальных границ, так как данные источники создаются с учетом универсальной международной практики и распространяются на субъектов предпринимательской деятельности вне зависимости от их юрисдикции.

В-седьмых, способ обеспечения реализации норм при государственно-правовом регулировании коммерческих отношений в информационной среде основывается на принудительной силе государства, и в случае нарушения норм при-

меняются виды наказания, предусмотренные нормами права страны. Правила lex informatica обеспечиваются самими участниками экономического оборота, исходя из сложившейся договорной практики, и в ситуации их неисполнения споры в большинстве случаев разрешаются в международных коммерческих арбитражах путем применения медиативных технологий и участия в переговорных процессах.

Таким образом, на основе проведенного анализа можно выделить характерные особенности, которые свойственны lex informatica:

– Lex informatica преследует цель сокращения пробелов в существующем праве;

– Lex informatica имеет особую структуру организации, которая отличается гибкостью и динамичностью развития в зависимости от условий современной экономической практики в информационной среде;

– Lex informatica обладает расширенным кругом субъектов, участвующих в правотворческом процессе, и меньшим формализмом при принятии решений;

– Lex informatica имеет трансграничный характер и распространяется за пределы территории более чем одного государства;

– Lex informatica носит автономный характер и не зависит от национально-правовых систем конкретных стран, но в то же время не ограничивает возможности субъектов предпринимательской деятельности к их обращению.

Из вышеизложенного следует, что правила lex informatica позволяют участникам коммерческих отношений в интернет-пространстве отказаться от применения материального и коллизионного права государства и воспользоваться существующими достижениями единообразной практики. Кроме того, в настоящий момент происходит фрагментация lex informatica и появляются такие формирования, как lex cryptographica, cyber law, e-merchant, law cyberspace и другие, которые призваны регулировать более узкие и специфичные области взаимоотношений субъектов права в киберпространстве.

Подводя итог, можно отметить, что современные международные коммерческие отношения в интернет-пространстве следует регулировать как с помощью традиционных способов, которыми обладает государство, так и посредством современных инструментов, основанных на актуальной практике трансграничных экономических правоотношений. Существующие нормативно-правовые источники не отменяют другие способы регулирования коммерческих отношений в киберпространстве, в свою очередь, альтернативные традиционному праву средства призваны упорядочить вновь возникающие области взаимодействия субъектов предпринимательской деятельности в современном цифровом обществе.

Список литературы

1. Karton J. Sectoral fragmentation of transnational commercial law. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3351880

2. Katsh M. E. Law in a Digital World. URL: https://digitalcommons.law.villanova.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2830&context=vlr

3. Polanski P. P. Towards a supranational Internet law. URL: https://media.neliti.com/media/publications/28672-EN-towards-a-supranational-internet-law.pdf

Н. А. Коровин,
ассистент,
Волгоградский государственный университет
(Волжский филиал)

ЦИФРОВЫЕ ТЕХНОЛОГИИ В ДЕЯТЕЛЬНОСТИ ОБЩЕСТВЕННОЙ ОРГАНИЗАЦИИ ТЕРРИТОРИАЛЬНОГО ОБЩЕСТВЕННОГО САМОУПРАВЛЕНИЯ

Аннотация. В статье рассматриваются предпосылки для использования цифровых технологий в деятельности общественных организаций территориального общественного самоуправления, затрагиваются вопросы договорного регулирования отношений, складывающихся по поводу применения указанных технологий. Рассматриваются различные виды цифровых технологий и цифровых устройств, а также виды договоров, применимых для регулирования отношений, складывающихся по поводу использования обозначенных устройств в деятельности общественных организаций территориального общественного самоуправления. Предлагается внесение изменения в законодательство, способствующее более эффективному вовлечению общественной организации территориального общественного самоуправления в гражданский оборот. Результаты, полученные в ходе исследования, могут быть применены для подготовки граждан, входящих в состав органов общественных организаций территориального общественного самоуправления. Выявлено, что существует потребность в более широком применении цифровых технологий для обеспечения эффективного осуществления гражданами территориального общественного самоуправления. Потребность граждан в комфортных (безопасных) условиях проживания обуславливает более широкое применение цифровых технологий и цифровых устройств на территории осуществления территориального общественного самоуправления, что достигается посредством взаимодействия указанного субъекта с другими участниками гражданского оборота, а также применением различных видов гражданско-правовых договоров.

Ключевые слова: цифровые технологии, некоммерческие организации, общественные организации, территориальное общественное самоуправление, гражданско-правовые договоры, договорное регулирование

DIGITAL TECHNOLOGIES IN THE ACTIVITIES OF PUBLIC ORGANIZATION OF TERRITORIAL PUBLIC SELF-GOVERNMENT

Abstract. The article discusses the prerequisites for the use of digital technologies in the activities of public organizations of territorial public self-government, touches upon the issues of contractual regulation of relations arising from the use of these technologies. Various types of digital technologies and digital devices are considered, as well as types of contracts applicable to regulate relations arising regarding the use of designated devices in the activities of public organizations of territorial public self-government. It is proposed to amend the legislation to facilitate more effective

involvement of the public organization of territorial public self-government in civil circulation. The results obtained during the study can be used to train citizens who are members of the bodies of public organizations of territorial public self-government. It has been revealed that there is a need for a wider use of digital technologies to ensure the effective implementation of territorial public self-government by citizens. The need of citizens for comfortable (safe) living conditions determines the wider use of digital technologies and digital devices in the territory of territorial public self-government, which is achieved through the interaction of the specified entity with other participants in civil circulation, as well as the use of various types of civil law contracts.

Keywords: digital technologies, non-profit organizations, public organizations, territorial public self-government, civil law contracts, contract regulation

Актуальность темы публикации связана с активным внедрением цифровых технологий во все сферы жизни общества и возникающей потребностью в надлежащем правовом регулировании этого процесса. Предприятия и организации при применении упомянутых технологий и электронных инструментов могут сделать свою деятельность наиболее эффективной [3. С. 89]. Как представляется, в деятельности общественной организации территориального общественного самоуправления тоже могут быть применены цифровые технологии и цифровые устройства.

О. В. Машевская в работе, посвященной исследованию цифровых технологий, обозначает цифровые технологии как технологии, в которых применяется современная техника с функцией записи определенного кода [5. С. 38]. Автор отмечает, что при расширяющихся технологических возможностях сказывается их влияние на различные сферы жизнедеятельности общества [5. С. 38]. Динамика развития цифровых технологий способствует тому, что они активно проникают в материальные объекты [4. С. 14]. Это способствует появлению новых цифровых платформ, систем и цифровых устройств, применение которых может решить ряд задач (проблем), стоящих перед гражданами, осуществляющими территориальное общественное самоуправление (далее – ТОС) в соответствии с положениями законодательства [8], регулирующего деятельность данной формы самоорганизации граждан. Согласно пп. 2 ч. 3 ст. 50 Гражданского кодекса Российской Федерации (далее – ГК РФ) [1] ТОС может являться некоммерческой организацией, созданной в такой организационно-правовой форме как общественная организация.

К целям деятельности общественной организации ТОС может относиться удовлетворение потребностей граждан, проживающих на территории ТОС, в формировании комфортной среды проживания, обеспечение благоустройства территории и решение других вопросов. Имея статус юридического лица, общественная организация ТОС посредством взаимодействия с другими участниками гражданского оборота может приобретать товары, выступать заказчиком услуги т. д. ТОС неоднократно становилось объектом внимания ученых, однако аспекты применения цифровых технологий в деятельности такой некоммерческой организации не были рассмотрены цивилистами в достаточной мере.

Рассмотрим предпосылки применения цифровых технологий и цифровых устройств в деятельности общественной организации ТОС. Ранее автором на-

стоящей публикации уже предпринималась попытка рассмотреть такой цифровой инструмент в деятельности ТОС, как интернет-сайт. Автор пришел к выводу, что предпосылкой возникновения потребности в использовании исследуемым субъектом собственного сайта в сети Интернет является существование запроса на должную осведомленность лиц, проживающих на территории осуществления ТОС, о деятельности самой некоммерческой организации и запроса на привлечение граждан к обсуждению проектов имеющихся инициатив и решению иных вопросов местного значения [2. С. 27]. Посредством применения договоров, способствующих созданию и использованию общественной организацией ТОС интернет-сайта, проявляется цифровизационный аспект частно-правового регулирования деятельности данной некоммерческой организации [2. С. 29].

Общественная организация ТОС посредством собственного сайта (или на площадках социальных сетей) может выносить на обсуждение лиц, проживающих на территории ТОС, инициативные проекты и ряд других вопросов, одобрение и принятие решений по которым допускается только в рамках проведения собрания (конференции) указанных лиц. Очевидно, что в условиях современного ритма жизни будет трудно обеспечить явку жителей для очного участия в собрании (конференции) и достичь необходимого кворума. Процедуру принятия решения упростило бы применение инструментов информационной платформы Единого портала государственных и муниципальных услуг (далее – «Госуслуги»). Так, к примеру, на «Госуслугах» до 10 сентября 2023 года Минцифры проводит всероссийское голосование за подключение сел и деревень к мобильному интернету. В онлайн-голосовании могут принять участие лица, имеющие подтвержденную учетную запись и зарегистрированные в регионе, в котором они могут выбрать соответствующий населенный пункт. Похожим образом участники собрания (конференции) ТОС могли бы выбрать варианты предлагаемых органом ТОС решений или одобрить (отклонить) инициативный проект.

Предполагается, что на повестке дня собрания (конференции) граждан могут решаться вопросы: об установке системы видеонаблюдения с применением IP-камер наблюдения на территории ТОС; об установке систем контроля и управления доступом на придомовую территорию или в подъезд многоквартирного дома. Упомянутые системы базируются на применении цифровых технологий. Так, современные IP-камеры имеются техническую возможность снимать, транслировать и хранить видео на удаленном сервере.

А. Н. Поликанин в статье, посвященной исследованию правовых вопросов при использовании видеонаблюдения, отмечает, что зачастую потребность в фиксации правонарушений является причиной установки камер [6. С. 251]. Таким образом, одной из предпосылок применения на территории осуществления ТОС систем видеонаблюдения является потребность жителей ТОС в обеспечении их безопасности. Нетрудно видеть, что решение собрания (конференции) ТОС может повлиять на применение договоров поставки и монтажа таких систем, инициирующих возникновение отношений по поводу приобретения, установки и возможной последующей эксплуатации указанного имущества.

В свою очередь, предпосылками применения на территории осуществления ТОС систем санкционированного доступа являются потребность жителей ТОС в обеспечении их безопасности, посредством ограничения доступа посторонним лицам (в подъезд жилого дома, на придомовую территорию). Упомянутые системы построены на цифровых технологиях, обеспечивающих распознавание личности и их видео-фиксацию. А. А. Туманов, рассматривая трудо-правовые аспекты применения системы контроля и управления доступом в организации, отметил, что исследуемая система рассматривается как источник сведений о событиях [7. С. 41]. Цивилисты отмечают, что создание инженерно-технических мероприятий создает препятствия для совершения несанкционированных проникновений [9. С. 112].

Подводя итоги публикации, можно сделать следующие выводы.

Во-первых, применение новых цифровых технологий и цифровых систем позволяет решить ряд задач, стоящих перед общественной организацией ТОС в целях удовлетворения потребностей граждан, проживающих на соответствующей территории.

Во-вторых, назрела острая необходимость в использовании возможностей информационного портала «Госуслуги» для обеспечения проведения онлайн-собраний (конференций) жителей ТОС.

В-третьих, решения граждан (органов) ТОС по поводу приобретения и использования цифровых устройств (система) на территории ТОС способствует вовлечению общественной организации ТОС в отношения с другими участниками гражданского оборота, а средством правового регулирования складывающихся отношений будет выступать гражданско-правовой договор.

Список литературы

1. Гражданский кодекс Российской Федерации (часть первая): Федеральный закон от 30.11.1994 № 51-ФЗ // СПС «КонсультантПлюс».

2. Коровин Н. А. Цифровизационный аспект договорного регулирования деятельности общественной организации территориального общественного самоуправления // Цивилист. 2023. № 4. С. 25-30.

3. Крылова Т. В., Трушкова Д. М., Фомина Н. И., Лелекова А. В., Сафатова К. С. Применение цифровых технологий в управлении предприятием // Инновационная экономика: перспективы развития и совершенствования. 2021. № 5(55). С. 88-92.

4. Ли Цзюнь, Юй Шуанюань. Актуальность внедрения процесса цифровизации в деятельность предприятий // Universum: экономика и юриспруденция. 2021. № 11(86). С. 13-18.

5. Машевская О. В. Цифровые технологии как основа цифровой трансформации современного общества // Вестник Полесского государственного университета. Серия общественных и гуманитарных наук. 2020. № 1. С. 37-44.

6. Поликанин А. Н. Правовые аспекты применения систем видеонаблюдения // Интерэкспо Гео-Сибирь. 2018. № 7. С. 250-253.

7. Туманов А. А. Система контроля и управления доступом в организации как электронное средство взаимодействия между работодателем и работником // Электронное приложение к Российскому юридическому журналу. 2015. № 5. С. 40-49.

8. Федеральный закон от 06.10.2003 № 131-ФЗ «Об общих принципах организации местного самоуправления в Российской Федерации» // СПС «КонсультантПлюс».

9. Шаронов С. А. Частноправовые аспекты антитеррористической защищенности объектов предпринимательской деятельности: на примере опасных производственных объектов // Вестник Московского университета МВД России. 2020. № 7. С. 108-113.

О. С. Лабабуева,
аспирант,
Санкт-Петербургский государственный экономический университет

О ПРАВОВОЙ ПРИРОДЕ ЦИФРОВОГО РУБЛЯ

Аннотация. В статье проведен сравнительный анализ цифрового рубля с цифровой валютой (криптовалютой) и безналичными денежными средствами, предпринята попытка определить правовую природу цифрового рубля. Согласно проведенному исследованию, цифровой рубль находится на стыке двух объектов права, обладающим обязательственной природой. Было предложено понятие цифрового рубля, а также предложено разграничить цифровое имущество и ввести в ГК РФ новую категорию.

Ключевые слова: цифровая валюта, криптовалюта, наличные денежные средства, безналичные денежные средства, национальное платежное средство, вещь, имущество

ABOUT THE LEGAL NATURE OF THE DIGITAL RUBLE

Abstract. The article provides a comparative analysis of the digital ruble with digital currency (cryptocurrency) and non-cash funds, an attempt is made to determine the legal nature of the digital ruble. So, according to the study, the digital ruble is at the junction of two objects of law, which have a binding nature. The concept of a digital ruble was proposed, and it was also proposed to distinguish between digital property and introduce a new category into the Civil Code of the Russian Federation.

Keywords: digital currency, cryptocurrency, cash, non-cash funds, national means of payment, thing, property

Развитие цифровой экономики во всем мире заставляет изменяться весь мировой уклад как в экономике, так и в праве. В связи с новыми мировыми тенденциями о развитии цифровых технологий в праве все чаще появляются новые объекты права, которые имеют отличные характеристики от привычных всем объектов, имеющих, в свою очередь, правовое регулирование. Новые объекты гражданского права обладают спорными характеристиками, поэтому в научных сообществах идут дискуссии о том, как правильно урегулировать данные объекты, к какой категории объектов их относить.

Российская Федерация старается не отставать от мировых тенденции о признании и регулировании новых цифровых объектов. Законодатель совместно с Центральным банком Российской Федерации (далее – ЦБ РФ) по примеру Китая решили создать собственную цифровую валюту. Так, совсем недавно были внесены изменения в гражданское законодательство о цифровом рубле. В частности, изменен перечень объектов гражданских прав в ст. 128 ГК РФ, к категории иное имущество добавлены цифровые рубли. Законодатель пошел по аналогии с цифровыми правами и признал цифровой рубль иным имуществом, а также согласно ст. 140 ГК РФ приравнял цифровой рубль к национальным валютам и разрешил осуществлять с ним расчеты. Тем не менее, как отмечает М. Д. Шапсугова, цифровой рубль не является разновидностью цифровых прав, а выступает в роли формы движения денег с экономической точки зрения и должен закрепляться в ГК РФ как цифровая валюта.

О. В. Вершинина отмечает в своей работе, что если рассматривать цифровой рубль, то его можно отнести к криптовалюте, так как по своей технической природе для выпуска в оборот требуется использовать специальные средства, такие как криптографические средства, специальные платформы, которые работают на блокчейн-технологии [3]. Однако автор справедливо указывает на существенное отличие цифрового рубля от криптовалюты. Так, она отмечает, что цифровой рубль, в отличие от криптовалюты, обеспечен активами ЦБ РФ.

Цифровой рубль по своей сути является централизованной валютой, а именно ее эмитентом выступает ЦБ РФ. Цифровая валюта, по задумке ЦБ РФ и законодателя, является обязательством ЦБ РФ, то есть существует конкретное лицо, которое создает и выпускает в оборот, в отличие от цифровой валюты, у которой нет конкретного лица, выпустившего ее. У цифровой валюты есть только владелец (обладатель), у которого цифровая валюта числится на балансе криптокошелька. Цифровой рубль, хоть и имеет схожую составляющую с цифровой валютой (криптовалютой), но приравнять их нельзя, однако, можно отнести к цифровым активам, так как цифровой рубль состоит из кода в системе блокчейн и схож с цифровыми правами. А также, благодаря ст. 140 ГК РФ, в которой законодатель указал, что рубль в наличной, в безналичной, либо в цифровой форме является средством платежа на территории РФ. Цифровая валюта не указана в данной статье, тем самым запрещена на территории РФ.

В поддержку мнения Т. В. Дерюгина дополнительно можно встретить мнения ученых, что цифровой рубль можно поставить в один ряд с безналичным и наличными деньгами. Так, ряд ученых [4] и представители ЦБ РФ полагают, что цифровой рубль рассматривается как третья валюта, как некое национальное денежное средство. По нашему мнению, цифровой рубль нельзя ставить в один ряд с безналичными денежными средствами, он имеет другую специфику, существенно отличающуюся от них. Цифровой рубль, несмотря на другую специфику, можно будет отнести к национальным денежным средствам, так как является централизованной валютой и эмитентом выступает ЦБ РФ в отличие от иных валют, в том числе цифровых.

Таким образом, можно сказать, что цифровой рубль является по своей сути новым национальным платежным средством, в основе которого лежит цифровой код в системе блокчейн и эмиссию которого осуществляет ЦБ РФ. С правовой точки зрения цифровой рубль можно отнести к иному имуществу и, учитывая его специфику, представляется возможным отнести его к цифровым активам. В своем роде цифровой рубль для государства новый способ контроля операций с деньгами внутри страны.

Законодатель, внеся изменения в ст. 128 ГК РФ, отнес цифровой рубль к иному имуществу. По задумке ЦБ РФ и законодателя цифровой рубль является обязательством ЦБ РФ, то есть на него распространяется обязательственно-правовой режим.

Е. М. Андреева считает, что в случае, если признать цифровой рубль иным имуществом, это повлечет за собой последствия. Во-первых, такое признание не позволит привести судебную практику к единообразию. Во-вторых, в связи с быстроизменяющимися экономическими отношениями не будет успевать давать разъяснения и толкования Верховный Суд РФ. Поэтому нарушенные права участников оборота цифрового рубля не могут быть эффективно защищены [1]. В связи с этим автор предлагает ввести новое понятие «цифровые вещи» в ГК РФ и отнести цифровой рубль к этой категории.

По нашему мнению, данное предложение является вполне правильным, это позволит отделить всем привычные вещи и имущество от новых цифровых категорий. Также можно отнести к этой категории и иные цифровые активы, такие как цифровые права (ЦФА, утилитарные цифровые права), цифровая валюта и т. п.

Л. Ю. Василевская считает, что неправильно относить цифровой рубль к вещам. По ее мнению, к вещам в силу юридической природы можно отнести только наличный рубль. Автор также придерживается мнения о том, что нельзя применить имеющиеся способы защиты обладателя цифрового рубля, так как цифровой рубль, как и криптовалюта (цифровая валюта), относится по своей правовой природе к безналичным денежным средствам [2].

По нашему мнению, цифровой рубль нельзя относить только либо к цифровой валюте, либо только к безналичным денежным средствам. Цифровой рубль находится на стыке двух объектов права, обладающих обязательственной природой, т. е. отнести к вещам его нельзя. Значит, возможно относить его к имуществу, к иному имуществу.

Перечень иного имущества слишком широк в ст. 128 ГК РФ и включает в себя в том числе и ценные бумаги. Однако это запутывает и не дает четкого ответа на вопрос о том, куда относить цифровой рубль. Как говорилось ранее, правильным и возможным представляется создать новую категорию объектов в ГК РФ «цифровые объекты» и отнести все цифровые вещи/имущество в этот перечень. Это позволит разграничить объекты, даст более широкое пояснение, чем же являются все цифровые объекты и куда их относить.

Таким образом, цифровой рубль требует большего внимания для исследования от ученых-цивилистов и законодателя для решения спорных вопросов.

Список литературы

1. Андреева Е. М. Общая характеристика и правовая природа цифрового рубля // Правовое регулирование цифровых денег: монография / Е. Н. Абрамова, Е. М. Андреева, А. Ю. Брагинец и др.; под ред. Е. Н. Абрамовой. М.: Юстицинформ, 2022. 236 с.

2. Василевская Л. Ю. Цифровой рубль: взгляд цивилиста на проблему // Lex Russica. 2023. № 1(194).

3. Вершинина О. В., Лабушева Я. Г., Султаниев И. С. Анализ возможностей и рисков введения в обращение цифровых валют центральных банков на примере «цифрового рубля» // Вестник Российского нового университета. Серия: Человек и общество. 2021. № 1. С. 51-60.

4. Турбанов А. В. Цифровой рубль как новая форма денег // Актуальные проблемы российского права. 2022. № 5. С. 73-90.

Ю. О. Лысаковская,
соискатель,
Академия управления при Президенте Республики Беларусь

РАСШИРЕНИЕ СФЕРЫ АГЕНТСКИХ ПРАВООТНОШЕНИЙ В СВЯЗИ С СОЗДАНИЕМ ТЕХНОЛОГИЧЕСКИХ ВОЗМОЖНОСТЕЙ ДЛЯ ДЕЛЕГИРОВАНИЯ АГЕНТСКОЙ ФУНКЦИИ ОБЪЕКТАМ ПРАВ – НОСИТЕЛЯМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Аннотация. Бурное развитие роботизации и расширение сферы применения искусственного интеллекта усиливают научную дискуссию о его правовом статусе по всему миру. Перед белорусской правовой системой стоит задача идентификации и институционализации искусственного интеллекта, определение порядка его разработки и использования. В статье анализируется правовое регулирование новых «цифровых» отношений в отдельных юрисдикциях, выявлены фундаментальные проблемы развития технологий искусственного интеллекта с точки зрения права, рассмотерны основные теории об искусственном интеллекте как об «искусственной личности» и определена возможность признания за искусственным интеллектом правового статуса субъекта права в целях идентификации и институционализации нового участника общественных отношений в правовой системе Республики Беларусь. Предлагается собственная концепция правового регулирования искусственного интеллекта в Республике Беларусь как электронного лица (агента).

Ключевые слова: искусственный интеллект, носитель искусственного интеллекта, электронное лицо, электронный агент, искусственная (электронная) личность, правовой статус искусственного интеллекта, конституционно-правовой статус искусственной личности, правосубъектность, ответственность, субъект права, объект права, философский зомби, кодекс поведения

EXTENSION OF THE SCOPE OF AGENCY RELATIONS IN CONNECTION WITH CREATION OF TECHNOLOGICAL POSSIBILITIES FOR DELEGATION OF AGENCY FUNCTION TO OBJECTS OF RIGHTS – CARRIERS OF ARTIFICIAL INTELLIGENCE

Abstract. The rapid grows of robotics and the extension of artificial intelligence enhances the scientific debate about its legal status worldwide. The Belarusian legal system is faced with the task of identifying and institutionalizing artificial intelligence and determining how to develop and use it. The Belarusian legal system is faced with the task of identifying and institutionalizing artificial intelligence, determination of its development and use regulation. The author analyzes the legal regulation of new "digital" relations in individual jurisdictions, identifies the fundamental problems of the development of artificial intelligence technologies from the legal point of view, considers the main theories on artificial intelligence as "artificial personality" and determines the possibility of recognizing artificial intelligence as a legal entity for the purpose of identifying and institutionalizing a new participant in social relations in the legal system of the Republic of Belarus. The author offers her own concept of legal regulation of artificial intelligence in the Republic of Belarus as an electronic person (agent).

Keywords: artificial intelligence, artificial intelligence device, electronic person, electronic agent, artificial (electronic) person, legal status of artificial intelligence, constitutional and legal status of artificial person, legal personality, liability, subject of law, object of law, philosophical zombie, ethic codes

Введение. В декабре 2022 г. крупнейший в СНГ белорусский оператор сети электрозарядок Malanka открыл первый супербыстрый зарядный комплекс в Минске – уникальный проект будущего, который включает и магазин безоператорной торговли (автономный супермаркет) [23].

Уникальное решение автономной сопутствующей торговли находится на стыке технологий компьютерного зрения, систем трекинга и искусственного интеллекта, а также весовых лотков, взаимодействие с которыми происходит через мобильное приложение. Модно и удобно. Мода на цифровизацию и технологии искусственного интеллекта набирает свои обороты, проникая все глубже в различные аспекты общественных отношений. Право не исключение. Автор также стремится быть в тренде и не обходит стороной концептуальные вопросы институционализации искусственного интеллекта как правовой категории.

По мнению авторитетного эксперта в области компьютерных технологий М. Бруссард, мир охватил «техношовинизм» – слепая вера, что технологии разрешат все проблемы цивилизации, но, только осознавая пределы компьютерных технологий, мы сможем распорядиться ими так, чтобы сделать мир лучше [3. С. 17; 31. С. 8]. Полагаю, данное утверждение справедливо применить и к праву: пока правоведы не определятся, какое место в системе права занимает искусственный интеллект, утверждать о том, что современная правовая система в полной мере соответствует потребностям постиндустриального общества, не представляется возможным. Объективно необходимо менять концептуальные подходы законодательств в целях «максимально эффективного покрытия» правового регулирования сферы инноваций.

Основная часть. Концепция правовой политики Республики Беларусь, вступившая в силу в июне 2023 г., среди основных направлений правовой политики в сферах гражданского, экономического (хозяйственного) законодательства выделяет среди прочих совершенствование законодательства с учетом современных экономических потребностей государства, общества и граждан и урегулирование вопросов обращения цифрового имущества и цифровых имущественных прав, применения искусственного интеллекта, робототехники, киберфизических систем, беспилотного транспорта [16]. Ряд документов принят белорусским законодателем в развитие Декрета Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики» [19], который предоставил резидентам Парка высоких технологий право на осуществление в установленном порядке деятельности в сфере искусственного интеллекта, создания систем беспилотного управления транспортными средствами, включая Закон Республики Беларусь «О защите персональных данных» [17].

Вместе с тем место искусственного интеллекта в национальной правовой системе Республики Беларусь до настоящего времени не определено, несмотря на тот факт, что Беларусь, как и иные государства, крайне заинтересована в разработке эффективного регуляторного поля для устойчивого развития сферы искусственного интеллекта.

В ряде стран уже сформирован комплекс нормативных правовых актов и (или) проектных документов, регулирующих отношения по разработке и использованию искусственного интеллекта и робототехники, например, Российская Федерация, США, страны Европейского союза, Япония, Южная Корея, Китай и др. [39].

Так, в Южной Корее эффективно работает Закон «О развитии и распространении умных роботов», в США и Канаде автором изобретения может являться только человек, не животное, не искусственный интеллект [29. С. 63–71], Германия на законодательном уровне возлагает ответственность за вред беспилотных транспортных средств с искусственным интеллектом на автопроизводителя [10. С. 9–28], в то же время в США есть проект закона, признающий искусственный интеллект беспилотного авто водителем [8. С. 65], а Европарламент уже с 2017 г. предлагает сложных автономных роботов в перспективе определять как обладающих правосубъектностью электронных лиц [32].

В целях формирования концепции национального правового регулирования искусственного интеллекта в Республике Беларусь рассмотрим существующие подходы к правовому регулированию в отдельных юрисдикциях.

Подход Европейского союза

Опыт Европейского Союза (далее – ЕС) многообразен и представляется наиболее комплексным. В 2018 г. были приняты Европейская этическая хартия об использовании искусственного интеллекта в системах правосудия 2018 г. (Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and their environment) [33], в 2020 г. – «Белая книга искусственного интеллекта – европейский подход к совершенству и доверию» (White Paper on Artificial Intelligence – A European approach to excellence and trust) [42] и ряд резолюций и нормативных актов, определяющих особенности правового режима использования искусственного интеллекта в отдельных сферах деятельности.

В апреле 2021 г. Европейской Комиссией был опубликован проект Регламента Европейского парламента и Совета ЕС о разработке гармонизированных правил об искусственном интеллекте (закон об искусственном интеллекте) и внесение изменений в некоторые законодательные акты Союза (Laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts), «данная инициатива стала ответом на запросы Европейского парламента и Европейского совета, которые неоднократно призывали к принятию законодательного решения по обеспечению хорошо функционирующего внутреннего рынка систем искусственного интеллекта, отмечая, что на уровне Евросоюза должна быть выработана соответствующая позиция как в отношении полезных сторон, так и в отношении рисков, связанных с искусственным интеллектом» [39].

Подход европейского законодателя предполагает установление нормативного правового регулирования только в отношении разработки и эксплуатации тех систем искусственного интеллекта, которые несут в себе наибольшие риски для общества, например, биометрическая идентификация, управление критической инфраструктурой, образование, трудоустройство, оказание государственных услуг, правоохранительная деятельность, управление миграцией, правосудие и демократические процессы (ст. 6 Регламента, Приложение III к Регламенту), в отношении иных систем достаточно разработки соответствующих кодексов поведения. Подлежит определенной критике, на наш взгляд, изъятие из сферы действия Регламента применение боевых роботов и интеллектуальных систем в военных конфликтах (п. 3 ст. 2 Регламента).

Таким образом, основными задачами ЕС в сфере искусственного интеллекта являются обеспечение равного распределения благ от использования данной технологии, минимизация рисков и построение стабильной, надежной и высокоэффективной индустрии искусственного интеллекта (правовая политика, основанная на ценностно ориентированном подходе).

Подход США

В США с 2021 г. вступил в силу Закон о национальной инициативе в области искусственного интеллекта (National Artificial Intelligence Initiative Act of 2020), согласно которому инициатива в области искусственного интеллекта должна обеспечить сохранение лидерства США в сфере развития искусственного интеллекта при обеспечении национальной безопасности [37].

S.2217 - FUTURE of Artificial Intelligence Act of 2017 (Закон о будущем искусственного интеллекта 2017 года) определяет ключевые признаки искусственного интеллекта, вводит такие термины, как «широкий искусственный интеллект» – будущий общенациональный искусственный интеллект, который будет иметь разумное поведение и быть, по крайней мере, настолько разумным, насколько может быть разумным человек в контексте когнитивного, эмоционального и социального поведения; «узконаправленный искусственный интеллект» – система искусственного интеллекта, занимающаяся задачами в определенной области, например, при осуществлении стратегической игры, языкового перевода, вождении беспилотного транспорта или распознавании изображений [41].

Китайский подход

Согласно принятому в 2017 г. Плану развития искусственного интеллекта нового поколения до 2030 г. Китайской Народной Республики (КНР), КНР должна стать мировым лидером в сфере искусственного интеллекта [36]. В рамках реализации столь амбициозной цели разработан целый ряд государственных и частно-государственных программ, направленных на повышение конкурентоспособности КНР в сфере компьютерного мышления, вместе с тем вопросы этического и правового регулирования использования систем искусственного интеллекта в КНР остаются открытыми [26. С. 590].

Подход Великобритании

В Великобритании с 2015 г. действует Стратегия цифровой экономики, согласно которой в стране создан Совет по искусственному интеллекту, определяющий направления развития искусственного интеллекта, осуществляющий государственную политику и контроль в данной сфере [36].

Подход Российской Федерации

В отличие от Республики Беларусь, в России принят «ключевой документ» в сфере правового регулирования искусственного интеллекта – Указ Президента Российской Федерации № 490 «О развитии искусственного интеллекта в Российской Федерации» (далее – Указ № 490) и Национальная стратегия развития искусственного интеллекта на период до 2030 года [18], определяющая основные принципы развития и использования технологий искусственного интеллекта: защита прав и свобод человека, безопасность, прозрачность, технологический суверенитет, целостность инновационного цикла, разумная бережливость, поддержка конкуренции, что в целом совпадает с принципами, отраженными в подходах законодателей США и ЕС.

Важным стратегическим документом является Национальная программа «Цифровая экономика Российской Федерации» [21]. В октябре 2021 г. в России презентован Национальный кодекс этики искусственного интеллекта, который рекомендательно устанавливает общие этические принципы и стандарты поведения участников отношений в сфере искусственного интеллекта [20].

На основании вышеизложенного можно констатировать:

1. Создание комплексного законодательства о разработке и использовании искусственного интеллекта находится на начальном этапе.

2. Стратегические документы и инициативные законопроекты могут выступить основой будущего правового регулирования новых общественных отношений в сфере разработки (создания) и использования технологий искусственного интеллекта.

3. Наличие национальной стратегии развития искусственного интеллекта не является необходимым условием разработки правового регулирования данных общественных отношений: только некоторые страны принимают специальные нормы непосредственного действия (законы, регламент и пр.) [24].

Справедливо отметить, что в целом вопросы правового регулирования искусственного интеллекта до настоящего времени должным образом не разрешены, что можно в определенной степени объяснить сложностью определения искусственного интеллекта как правовой категории.

По нашему мнению, искусственный интеллект можно рассматривать в качестве некого электронного (программного) агента лица, им владеющего, это часть новой экосистемы – интернета вещей [12], объективная реальность, существенно расширяющая сферу агентских правоотношений как частного, так и публичного порядка и требующая институционализации в национальных правовых системах, равно как и в международном праве.

Для формирования нормы законодательного акта, регулирующего взаимоотношения искусственного интеллекта как электронного агента и его владельца, как нам видится, необходимо разрешить следующие проблемы:

– отсутствие общепринятого определения понятия «искусственный интеллект»;

– нечеткость границ между ответственностью владельца искусственного интеллекта и самого искусственного интеллекта (электронного агента).

Примером вышесказанного является упомянутый в начале автономный супермаркет, который является технически сложным устройством, способным самостоятельно принимать решения (отпуск товара, расчеты и пр.) в интересах его владельца (принципала). Очевидно, что такие решения могут иметь негативные последствия для потребителя.

Возвращаясь к вопросу о делегировании агентской функции объектам прав – носителям искусственного интеллекта, необходимо определить правовой статус и правовой режим искусственного интеллекта в национальной правовой системе.

Большинство правоведов посвящают исследования вопросу юридической и (или) фактической (физической) ответственности искусственного интеллекта: кто несет ответственность за причиненный им вред (разработчик, правообладатель, продавец, пользователь или третьи лица). В этой связи возникает правомерный вопрос: является ли искусственный интеллект объектом или субъектом права? Действующее законодательство Республики Беларусь сегодня определенных ответов на данный вопрос не дает.

В российском научном сообществе за последние нескольких лет опубликовано значительное количество публикаций, посвященных искусственному интеллекту, в том числе правовому регулированию: Н. В. Антонов, И. Р. Бегишев, С. Б. Бальхаев, Ж. А. Гаунов, Ю. А. Тихомиров, П. Ролинсон, Е. Н. Ирискина, А. В. Тюлин, Е. А. Моргунова, И. А. Филипова, Б. А. Шахназаров и др. [5, 7, 8, 10, 11, 14, 15, 22, 24, 25–29].

Особого внимания, на наш взгляд, заслуживает монография «Теория правового регулирования искусственного интеллекта, роботов и объектов робототехники в Российской Федерации» об определении места искусственного интеллекта и роботов в системе общественных отношений:

– искусственный интеллект и роботы признаются объектами права, что соответствует сложившейся догме об объектах и субъектах права;

– робот – юридическое лицо;

– робот – человек, то есть приравнивается к физическому лицу как субъекту права;

– робот – электронное лицо (агент) [27].

Среди белорусских правоведов вопросы правового положения и правового режима искусственного интеллекта поднимали представители белорусской школы хозяйственного права профессор Н. Л. Бондаренко, Ю. Г. Конаневич, Ю. О. Лысаковская [1, 12]. Так, Н. Л. Бондаренко и Ю. Г. Конаневич предложили концептуально новый подход к институционализации нестандартных по своей природе объектов, содержащих элементы объекта интеллектуальной собственности (тот же искусственный интеллект) в рамках правовой системы Республики Беларусь [1]. Авторы отмечают в своем исследовании, что в скором времени «признаваемый в правовой науке и в праве на сегодняшний день круг субъектов общественных отношений претерпит довольно значительную трансформацию» [1. С. 7] (с чем нельзя не согласиться в свете развития технологий и появления совершенно новых общественных отношений), и предлагают уникальный концепт институционализации объектов публичной идентификации в качестве нового типа объектов интеллектуальной собственности, позволяющий создать универсальный правовой и общесоциальный механизм идентификации и имплементации искусственного интеллекта в систему общественных отношений. Искусственный интеллект, точнее носители данной технологии, относится к новому типу объектов публичной идентификации [1. С. 9].

При этом, как верно отметили в своем исследовании Н. Л. Бондаренко, Ю. Г. Конаневич [1], Ю. О. Лысаковская [12] вне зависимости от подхода к определению правового статуса искусственного интеллекта и робота в системе общественных отношений (объект или все же субъект) ставит перед научным сообществом и непосредственно перед законодателем проблему идентификации отдельно взятой единицы искусственного интеллекта. В случае признания искусственного интеллекта как объекта права, необходимо наделить такой объект «именем», поскольку функционирует такой объект с определенной степенью автономности от правообладателя и производит определенное материальное или нематериальное благо. Очевидно, что существующая система права интеллектуальной собственности не содержит соответствующего объекта интеллектуальной собственности.

В случае признания за искусственным интеллектом правового статуса субъекта возникает аналогичная проблема: необходимо указанный субъект «поименовать» среди прочих существующих традиционных субъектов общественных отношений.

В случае признания государством робота субъектом общественных отношений [2], правового режима объекта публичной идентификации, возможно четкое и эффективное разграничение родового, институционального, функционального и индивидуального правового статуса физических лиц и роботов, юридических лиц (организаций без статуса юридического лица) и роботов (в зависимости от концепции субъективации искусственного интеллекта, которую изберет конкретный законодатель).

Автор является сторонником концепции субъективации технологии искусственного интеллекта (ее материальных носителей) в качестве «электронного лица (электронного агента)» физического или юридического лица [12, 13]. Указанная концепция позволит создать абсолютно новую категорию субъектов обществен-

ных отношений – субъектов агентских правоотношений как нового типа правоотношений. Разделяем позицию Н. Л. Бондаренко и Ю. Г. Конаневича о том, что идентификация искусственного интеллекта на основе института объектов публичной идентификации позволит разрешить проблему с правоспособностью, дееспособностью и деликтоспособностью робота [1. С. 9].

Справедливости ради следует отметить, что, ведя речь о правовом регулировании разработки и использования технологий искусственного интеллекта в Республике Беларусь, равно как и в ряде иных правовых систем, ошибочно утверждать, что данная проблематика находится в неком правовом вакууме. Существующие правовые институты (право интеллектуальной собственности, например, договорное право, деликтное и пр.) позволяют определенным образом регулировать новый тип общественных отношений с участием искусственного интеллекта как объекта [12. С. 454].

При этом уже сегодня становится очевидным, что традиционные институты не позволяют охватить весь спектр новых общественных отношений, эффективно регулировать их в целях содействия технологическому развитию Республики Беларусь, обеспечению надлежащего уровня защиты прав и свобод человека и гражданина, сохранению фундаментальных гуманитарных ценностей при обеспечении повышения благосостояния страны в целом и граждан и бизнеса в частности.

До настоящего времени не существует единого понятия искусственного интеллекта, в целом данная научная категория представляется нам в большей степени дискуссионной [28]. Фактически программисты противопоставили искусственному интеллекту интеллект естественный (человека и иных живых организмов).

Так, Ю. А. Цветков как критик технологического подхода отмечает, что «программисты пытаются искусственно воспроизвести свои представления об интеллекте, а не то, что есть интеллект в действительности с точки зрения психологии, предметом изучения которой он является [28. С. 16].

Великий философ прошлого века К. Ясперс определял интеллект как «совокупный умственный потенциал человека», выделял: предпосылки интеллекта (память, утомляемость, речевой аппарат и т. д.); багаж знаний и связанную с ним способность к обучению, которую также предлагал отделять от чистого интеллекта; и интеллект в собственном смысле этого слова [30. С. 266–268].

Американский психолог, известный как автор понятия «множественный интеллект», Г. Гарднер определяет интеллект следующим образом: «Вообще интеллект можно определить как нейронный механизм или компьютерную систему, которая генетически запрограммирована реагировать на определенные виды внутренней или внешней информации» [34. С. 69], то есть допускает следующее толкование: так как интеллект – это всего лишь сложно устроенная вычислительная система, то постоянное совершенствование ее искусственного аналога когда-нибудь сравняется со своим естественным прототипом и даже превзойдет его.

Так что же собой представляет искусственный интеллект как правовая категория?

Принимая во внимание нашу позицию касательно правового статуса искусственного интеллекта (его носителей) как электронного лица (электронного агента), обратимся к философским теориям об искусственной личности, детальный анализ которых проведен в исследовании О. Н. Гурова и А. В. Шерстова [5].

Так, известный российский мыслитель, доктор философских наук А. Ю. Алексеев определяет понятие «философский зомби» относительно «личности» когнитивно-компьютерной системы, что идентично понятию «искусственная личность», и представляет собой в широком смысле «систему, не обладающую сознанием, но при этом с точки зрения поведения, выполняемых функций, по внешнему виду неотличимо или очень похоже на существо, обладающее сознанием» [5. С. 63]. Авторы отмечают также «зомбифилов», которые применительно к искусственному интеллекту допускают, что создание функционально идентичных двойников, не обладающих сознанием, возможно. «Антизомбисты» признают абсурдной идею о возможности существования зомби как такового. При этом определенную ясность в данную проблему, по мнению О. Н. Гурова, вносят «нейтралы», утверждая, что компьютерная модель должна включать модуль «псевдосознания», аналогичного человеческому сознанию. При этом существуют и «азомбисты», которые игнорируют сам вопрос о «сознании» искусственных систем, так как их идентификация не нужна.

В настоящее время философами разработаны следующие основные модели искусственной личности [5. С. 63-65]:

Модель 1. Искусственная личность как имитация естественной личности (азомбисты). Искусственный субъект не отличается от естественного: личности похожи не только по структуре и функционированию внешних видимых систем (физической, физиолого-анатомической, вербально-коммуникативной и пр.), но и внутренней духовной системы, которая отвечает за абстрактные понятия, присущие эмоциональной и чувственной, рефлексивной стороне человека (например, «ответственность», «право» и т. д.).

Модель 2. Искусственная личность как модель естественной личности. Наличие у искусственной личности комплекса «псевдосознания», который используется с целью манипуляции и управления так называемыми знаниями и, конечно же, данными, оперируемыми интеллектуальной системой.

Модель 3. Искусственная личность как воспроизведение естественной личности (антизомбисты). Искусственный интеллект воспроизводит все существующие феномены, свойственные человеческому сознанию, посредством реализации сложной функциональной зависимости нейрофизиологических кодов субъективной реальности от субстрата, инвариантного по отношению к физиологической структуре человеческого мозга. Например, Д. И. Дубровский определяет важное условие для возникновения искусственной личности – «Я», которое и формируют личность: генетический и биографический уровни. При этом, как отмечают европейские ученые Джозеф Гуггемос (Josef Guggemos), Стефан Сондереггер (Stefan Seufert) и Сабина Сеуферт (Sabine Seufert) в работе «Робот-гуманоид с индивидуальностью?» (“A humanoid robot with personality?”), генетический уровень можно легко подделать или воспроизвести, в то время как

биографический уровень – это опыт, который необходимо получить, осмыслить и сохранить [5. С. 64].

Модель 4. Искусственная личность – как создание (формирование) «сверхличности». По мнению Д. Денетта, создает такие качества (явления), которые не имеют аналога у естественной личности (идея «сверхличности») [5. С. 65].

Как отмечают Гуров и Шерстов, дать «точное и единое определение искусственной личности» на данном этапе не представляется возможным, поскольку до сих пор не существует единого, общепризнанного понимания феномена человеческой личности и существует многообразие представлений о способах компьютерной реализации персонологических феноменов [5. С. 65].

В науке выделяют два основных подхода к определению искусственной личности [5. С. 66–67]:

1. Это робот с псевдосознанием – обладатель функционального подобия субъективного сознания реальности, присущего человеку (идея антропопатизма, согласно которой искусственная личность наделяется свойствами человеческой психики, но робот никогда не станет человеком, то есть естественной личностью [5. С. 66]. По мнению сторонников данного подхода, результат формального копирования опыта лишен основной составляющей – чувств и эмоций, позволяющих человеку фиксировать память, делать выводы и оценивать полученный опыт посредством морального удовлетворения от результата, в то время как машина способна только имитировать чувства.

2. Это сложная экспертная система, обладающая механизмами «чувствования». Подход сопряжен с проблемой моделирования «смысла»: если машина «понимает», то что для нее «смысл»? Сторонники подхода приводят в пример принцип работы чатбота Tay от Microsoft, который обучается и тренируется на основе сообщений пользователей и генерирует на их основе новые реплики. Впоследствии разработчик признал, что недооценил социальный аспект при разработке: чат-бот не может «мыслить», не способен отфильтровать негативную информацию и отделить ее от нейтральной или позитивной. То есть нынешние прототипы искусственной личности не являются автономными в полном смысле этого слова, им все еще нужен модератор (оператор) в отличие от человека [5. С. 67].

Таким образом, часть российского философского сообщества констатирует необходимость формирования нового научного языка на пересечении философской антропологии, философии сознания, философии технологии, философии искусственного интеллекта на базе изучения этических проблем, возникающих в сфере искусственного интеллекта [5. С. 73].

В отличие от философии в российской юридической литературе сегодня можно выделить ряд предложений по определению искусственного интеллекта.

Искусственный интеллект – «искусственная сложная кибернетическая компьютерно-программная система с когнитивно-функциональной архитектурой и собственными или релевантно доступными вычислительными мощностями, обладающая свойствами субстантивности (включая определенную правосубъектность и автономность), элаборативной операциональностью, высокоуровневыми возможностями восприятия и моделирования окружающих образов, саморефе-

рентно принимающую и реализующую решения, анализирующую и понимающую свое поведение и опыт, самостоятельно моделирующую и корригирующую алгоритмы действий, воспроизводящую когнитивные функции (включая связанные с глубинным самообучением), способную самореферентно адаптировать свое поведение и осуществлять омологацию себя и подсистем» [14. С. 1095–1096].

Искусственный интеллект – система, обладающая следующими характеристиками: 1) факультативностью аппаратного воплощения; 2) способностью анализировать окружающую среду; 3) наличием определенной автономности в функционировании; 4) наличием способности накопления опыта, его оценки и реализации задачи самообучения; 5) наличием «интеллектуальности», описываемой через категории «разумности», «рациональности» или способности «мыслить, как человек» или «действовать, как человек», во всех или в определенных обстоятельствах» [14. С. 1095–1096].

Зарубежные ученые-правоведы, как правило, определяют искусственный интеллект как нечто прикладное: технология или технологии и методы [14. С. 1095], в единичных случаях рассматривают возможность искусственного интеллекта выступать субъектом конституционного права. Лоуренс Соулум (Lourence Solum) считает, что «искусственные интеллекты (объекты с искусственным интеллектом) и даже объекты с полноценным искусственным интеллектом (киберсубъекты) не являются людьми и не могут позиционироваться в качестве аналогичных или тождественных людям. Это наиболее прямой из всех аргумент: можно утверждать, что только люди могут обладать конституционными правами» [40. Pp. 1258–1259]. В отечественной науке эта проблема не разработана.

Следовательно, для признания искусственного интеллекта субъектом права первоначально необходимо определить конституционно-правовой статус нового субъекта.

В законодательстве Великобритании, США и других странах искусственный интеллект определяется через конкретные методы и технологии, обеспечивающие результаты, сопоставимые с результатами человеческой интеллектуальной деятельности [36, 37]. При этом носители искусственного интеллекта классифицируются по степени автономности, на основании чего законодатель распределяет юридическую ответственность между самим носителем и его правообладателями, пользователями, создателями и др. [11. С. 106].

Проведенное исследование правового регулирования и институционализации искусственного интеллекта и роботизации в ряде юрисдикций позволяет сделать следующие выводы.

1. Объективно существует новый тип отношений по разработке (созданию) и использованию искусственного интеллекта, роботов и робототехники.

2. Отсутствие эффективного нормативного правового регулирования новых типов общественных отношений приводит к ряду проблем:

2.1. Отсутствие общепринятого понятия искусственного интеллекта, робота.

2.2. Отсутствие идентификации искусственного интеллекта в системе общественных отношений.

3. Безопасная разработка и использование технологий искусственного интеллекта требуют создания эффективного правового регулирования новой цифровой сферы общественных отношений, которые де факто уже существуют.

Заключение. Результаты проведенного анализа позволяют констатировать, что текущий уровень развития технологий требует существенной трансформации сложившейся правовой догмы.

До настоящего времени ряд фундаментальных проблем правового регулирования искусственного интеллекта в правовой системе Республики Беларусь, как и в ряде иных государств, остается неразрешенным: искусственный интеллект не идентифицирован (не определен его правовой статус), не определен правовой режим его использования в рамках публичных и частных отношений.

Национальная правовая система с традиционными институтами договорного, деликтного права, права интеллектуальной собственности определенным образом позволяет обеспечивать защиту носителя искусственного интеллекта как любого другого объекта права, но не как субъекта.

Искусственный интеллект уже выступает участником правоотношений как нечто, способное имитировать интеллект человека, самообучаться и принимать определенные решения, в том числе на основании встроенных алгоритмов без получения данных от человека (саморазвивающиеся системы).

В случае, когда искусственный интеллект выступает участником договорных отношений (стороной электронного договора купли-продажи, например), требуется идентифицировать его правовой статус, включая деликтоспособность.

В связи с чем разработка детального правового регулирования искусственного интеллекта и роботизации является приоритетом государственной политики большинства стран мира, что позволит трансформировать ценности и правила в соответствии с новой цифровой реальностью для дальнейшего развития технологий исключительно на пользу и во благо человечеству.

Нами предлагается следующая концепция правового регулирования искусственного интеллекта в Республике Беларусь:

1. Принять специальный акт законодательства (специальные нормы регулирования) – Закон Республики Беларусь «Об искусственном интеллекте».

2. Определить правовой статус искусственного интеллекта в законе как электронного лица (электронного агента) – субъекта общественных отношений, признав за ним правосубъектность, т. е. отождествить с человеком как субъектом права.

3. Определить правой режим разработки и использования искусственного интеллекта.

4. Внести изменения в Конституцию Республики Беларусь, закрепив в ней конституционно-правовой статус искусственного интеллекта – «искусственная (цифровая) личность» в отличие от правового статуса человека – «личность».

4. Идентифицировать носитель технологий искусственного интеллекта в законе.

5. Институционализировать агентские отношения в рамках кодификации хозяйственного законодательства Республики Беларусь: глава «Агентирование» Хозяйственного кодекса Республики Беларусь.

Список литературы

1. Бондаренко Н. Л., Конаневич Ю. Г. Объекты публичной идентификации как новый тип объектов интеллектуальной собственности // Интеллектуальная собственность в Беларуси. 2023. № 2. С. 6-15.

2. Бегишев И. Р. Искусственный интеллект и робот как правовые категории // Безопасность бизнеса. 2020. № 6. С. 32-36.

3. Бруссард М. Искусственный интеллект: пределы возможного. М., 2020. 362 с.

4. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 № 14-ФЗ // СПС «КонсультантПлюс».

5. Гуров О. Н., Шерстов А. В. Проблемы управления искусственной личностью // Исследования в цифровой экономике. 2023. № 1. С. 61-89.

6. Декрет Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики» // СПС Ilex.

7. Зырянов И. А. К вопросу о введении киберответственности искусственного интеллекта // Конституционное и муниципальное право. 2023. № 5. С. 53-58.

8. Ирискина Е. Н., Беляков К. О. Правовые аспекты гражданско-правовой ответственности за причинение вреда действиями робота как квазисубъекта гражданско-правовых отношений // Гуманитарная информатика. 2016. Вып. 10. С. 65-95.

9. Кодекс Республики Беларусь от 07.12.1998 № 218-З «Гражданский кодекс Республики Беларусь» // СПС Ilex.

10. Кирпичников Д. В. Искусственный интеллект как правовая категория: доктринальный подход к разработке дефиниции // Актуальные проблемы экономики и права. 2020. Т. 14, № 1. С. 79-91. EDN ESEBKI

11. Крысанова-Кирсанова И. Г., Трушина И. О. Правовой статус искусственного интеллекта // Вестник экономической безопасности. 2022. № 2. С. 104-107.

12. Лысаковская Ю. О. Агентирование и искусственный интеллект: перспективы развития // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции. В 6 т., Казань, 23 сентября 2022 года / под ред. И. Р. Бегишева [и др.]. Т. 2. – Казань: Познание, 2022. С. 453-460. EDN SZNZMD

13. Лысаковская Ю. О. Агентские отношения как основа функционирования системы странового маркетинга. Страновой маркетинг: монография / под ред. Н. Л. Бондаренко. Минск: Ковчег, 2022. 652 с.

14. Минбалеев А. В. Понятие «искусственный интеллект» в праве // Вестник Удмуртского университета. Серия «Экономика и право». 2022. № 6. С. 1094-1099.

15. Моргунова Е. А., Шахназаров Б. А. Право интеллектуальной собственности в условиях развития новых технологий: монография. М.: Норма, ИНФРА-М, 2023. 152 с.

16. Указ Президента Республики Беларусь от 15.09.2021 № 348 «О Государственной программе инновационного развития Республики Беларусь на 2021–2025 годы» // СПС Ilex.

17. Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных» // СПС Ilex.

18. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // СПС «КонсультантПлюс».

19. Декрет Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» // СПС Ilex.

20. Официальный сайт Комиссии по реализации Кодекса этики в сфере искусственного интеллекта. URL: https://ethics.a-ai.ru

21. Официальный сайт Национальной программы «Цифровая экономика Российской Федерации». URL: https://digital.ac.gov.ru

22. Перькова В. В. Носители искусственного интеллекта и их правовые положения // Юридическая наука. 2023. № 3.

23. Петрович В. В Минске открылся супербыстрый зарядный комплекс с 8 станциями и автономным супермаркетом. URL: https://auto.onliner.by/2022/12/27/superbystryj-zaryadnyj-kompleks

24. Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и робототехники: история, современное состояние и перспективы развития: монография / В. В. Архипов и др.; под общ. ред. В. Б. Наумова СПб.: НП-Принт, 2020. 260 с.

25. Ролинсон П., Ариевич Е. А., Ермолина Д. Е. Объекты интеллектуальной собственности, создаваемые с помощью искусственного интеллекта: особенности правового режима в России и за рубежом // Закон. 2018. № 5. С. 63-71.

26. Струкова П. Э. Искусственный интеллект в Китае: современное состояние отрасли и тенденции развития // Вестник Санкт-Петербургского университета. Востоковедение и африканистика. 2020. Т. 12, Вып. 4. С. 588-606.

27. Теория правового регулирования искусственного интеллекта, роботов и объектов робототехники в Российской Федерации: монография / Г. Ф. Ручкина [и др.]; под ред. Г. Ф. Ручкиной. М.: Прометей, 2020. 294 с.

28. Филипова И. А., Коротеев В. Д. Будущее искусственного интеллекта: объект или субъект права? // Journal of Digital Technologies and Law. 2023. № 2. С. 5-32.

29. Юридическая концепция роботизации: монография / Н. В. Антонова, С. Б. Бальхаева, Ж. А. Гаунова и др.; отв. ред. Ю. А. Тихомиров, С. Б. Нанба. М.: Проспект, 2019. 240 с.

30. Ясперс К. Общая психопатология. М., 1997. 365 с.

31. Broussard M. Artificial Unintelligence: How Computers Misunderstand the World. The MIT Press, 2018. 237 p.

32. Civil Law Rules on Robotics European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) (2018/C 252/25). URL: https://eur-lex.europa.eu

33. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. URL: https://rm.coe.int

34. Gardner H. Frames of Mind: The Theory of Multiple Intelligence. 3rd edition. Basic Books, 2011. 528 p.

35. Guidelines for National New Generation Artificial Intelligence Innovation and Development Pilot Zone Construction Work / The State Council of the People's Republic of China. URL: http://www.gov.cn

36. Industrial Strategy. Building a Britain fit for the future. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/664563/industrial-strategy-white-paper-web-ready-version.pdf

37. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools. URL: https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf

38. National AI policies & strategies. URL: https://oecd.ai

39. Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts. URL: https://eur-lex.europa.eu

40. Solum L. B. Legal Personhood for Artificial Intelligences // North Carolina Law Review. 1992. Vol. 70(4). P. 1258-1259.

41. S.2217 - FUTURE of Artificial Intelligence Act of 2017. URL: https://www.congress.gov/bill/115th-congress/senate-bill/2217/committees

42. White Paper on Artificial Intelligence - A European approach to excellence and trust. URL: https://ec.europa.eu

Н. А. Малышева,
кандидат юридических наук,
Московский университет Министерства внутренних дел
Российской Федерации имени В. Я. Кикотя

НОВЫЕ ГРАЖДАНСКО-ПРАВОВЫЕ РЕЖИМЫ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. В статье рассматриваются две основные проблемы гражданского права в условиях цифровизации: 1) правосубъектность искусственного интеллекта; 2) создание результатов интеллектуальной деятельности с использованием технологии искусственного интеллекта. На основании исследования сделаны выводы об «искусственности» существования первой и о необходимости решения второй проблемы в плоскости установления нового гражданско-правового режима. Выявлены особенности рассматриваемого правового режима.

Ключевые слова: цифровизация, искусственный интеллект, правовой режим, принципы гражданского права, субъекты гражданского права, цифровые технологии, нейросеть

NEW CIVIL LAW REGIMES IN THE CONTEXT OF DIGITAL TRANSFORMATION

Abstract. The article deals with two main problems of civil law in the context of digitalization: 1) legal personality of artificial intelligence; 2) creation of the results

of intellectual activity using artificial intelligence technology. The author comes to the conclusion about the «artificiality» of the existence of the first and the need to solve the second problem in the plane of establishing a new civil law regime. The article reveals the features of the legal regime under consideration.

Keywords: digitalization, artificial intelligence, legal regime, principles of civil law, subjects of civil law, digital technologies, neural network

Современные условия развития гражданского оборота диктуют новые правила формирования регуляторов частноправовых отношений. Внедрение цифровых технологий в повседневную жизнь общества привело к резкому возрастанию роли норм частного права в регулировании общественных отношений. Л. Ю. Василевская справедливо отмечает, что появление в имущественном обороте цифровых объектов и различных технологий свидетельствует о мультисодержательном характере сферы частноправового регулирования [2. С. 105]. Это означает, что в границы частного права укладываются сложные бизнес-связи, киберпространство, цифровые платежные системы и многое другое. Указанные обстоятельства усложняют систему гражданско-правовых отношений, вносят в них ранее незнакомые праву элементы, что обусловливает необходимость адаптации существующих правовых норм под объективные жизненные обстоятельства.

Процессы цифровизации, безусловно, оказывают влияние на правовую реальность, в результате чего нормы права и другие юридические конструкции подвергаются множественным изменениям. Однако носят ли такие изменения фундаментальный характер и все ли явления заслуживают пристального внимания для изучения? По мнению А. И. Клименко тренд цифровизации оказывает сильное влияние на развитие общественных отношений, но результаты такого влияния нельзя назвать фундаментальными изменениями [6]. Соглашаясь с мнением профессора, считаем необходимым обратиться к анализу понятия «фундаментальный». Многие юридические исследования последних лет активно оперируют данным понятием [4, 11], но не все исследователи обращаются к семантике слова. В словаре С. И. Ожегова «фундаментальный» означает «прочный, основательный, глубокий» [12]. В связи с этим можно сказать, что фундаментальные изменения должны затрагивать самые глубинные основы гражданского права. По нашему мнению, в настоящее время достижения цифровой эпохи еще не достигли такого уровня, который бы оказывал влияние на базовые гражданско-правовые институты.

Автор статьи не склонен умалять «заслуги» цифровизации, а пытается выявить те сущностные аспекты этого правового явления, которые в действительности имеют значение для науки гражданского права и правоприменения. Для этого предлагаем выявить и проанализировать наиболее часто встречаемые проблемы, которые являются предметом рассмотрения научных статей, диссертаций и монографий.

1. Наиболее яркое отражение проблема цифровизации нашла в мнениях ученых о возможностях признания технологии искусственного интеллекта субъектом гражданских правоотношений [1; 5]. В трудах ученых можно встретить и гибридный концепт правосубъектности «электронное лицо», центральной идеей кото-

рого является специфическое участие искусственного интеллекта (далее – ИИ) в гражданских правоотношениях [8. С. 30–32]. Так или иначе вопросы правосубъектности активно поднимались и поднимаются научным сообществом. Однако, опираясь на действующие принципы гражданского права, являющиеся идейными началами правовой отрасли, автор приходит к выводу о нецелесообразности рассуждений на тему трансформации института правосубъектности.

Аргументация такого вывода строится на двух важных постулатах: во-первых, традиционные истоки гражданского права признают участниками гражданских правоотношений физических и юридических лиц, публично-правовые образования; во-вторых, согласно п. 2 ст. 1 Гражданского кодекса Российской Федерации (далее – ГК РФ), физические и юридические лица приобретают и осуществляют свои гражданские права своей волей и в своей интересе. Из этого следует, что все участники гражданских правоотношений обладают признаком воли, который и позволяет им действовать в своем интересе. Какой же будет интерес у искусственного интеллекта (даже у самого развитого)? Интерес – это осознанная потребность, а технология, лишенная сознания, на наш взгляд, может действовать лишь в интересах своего создателя либо лица, который определил конкретные параметры задания.

Возможно, в будущем технология ИИ будет способна распоряжаться своей волей и действовать в своем интересе, однако сегодня размышления о правосубъектности ИИ представляются автору преждевременными, необоснованными и противоречащими логике базовых начал гражданского права. Справедливо отмечает А. В. Габов, что любые изменения в систему не должны нарушать ее логику, а значит, быть конструктивными и соответствовать законам существования самой системы [3. С. 63]. Если в систему будет внедрен элемент, чуждый ей, то система может не справиться и начать деградировать.

2. Вторая важная проблема тренда цифровизации кроется в институте права интеллектуальной собственности, и, по мнению автора, именно она связана с созданием новых правовых режимов.

Перед тем как раскрыть проблему в обозначенной сфере, важно обратиться к последним достижениям использования технологии ИИ. Актуальной темой для обсуждения является написание дипломной работы американской нейросетью ChatGPT [9]. Кроме того, нейросети также активно используются онлайн-платформами для расширения возможностей создателей музыкального контента (Mubert, Juxebox, Soundraw и т. д.) [9], для создания видеосюжетов, картин и пр. Указанные аспекты указывают на необходимость определения доли участия гражданина в создании результатов интеллектуальной деятельности (далее – РИД) и правовых притязаний на объект творчества.

В связи с этим в литературе встречается мнение о возможности экстраполяции характеристик субъекта творческой деятельности применительно к технологии ИИ [13. С. 21]. С одной стороны, приведенные выше автором аргументы не позволяют признать ИИ субъектом правоотношений. С другой – по справедливому замечанию В. О. Калятина, «традиционные подходы регулирования прав на РИД ослабляют охрану объектов, в создании которых человек не проявил явной творческой активности» [7. С. 27].

Рассуждения исследователей зачастую лежат именно в плоскости степени проявления активности человека при создании результата творческой деятельности, в определении его вклада. Однако, по нашему мнению, исследование вопроса под призмой степени проявления творчества является неэффективным по двум причинам: во-первых, указанные размышления вновь лежат в плоскости наделения правосубъектностью ИИ; во-вторых, включение в понятие «проявление творчества» элемента духовности исключает возможность правовой охраны РИД, созданных с использованием ИИ.

Таким образом, решение такой проблемы кроется не в расширении субъектного состава участников правоотношений, а в дополнении существующих правовых режимов новым, который предлагаем назвать «РИД, созданные с применением технологии ИИ». Изменения перечня объектов гражданских прав в данном случае не потребуется, поскольку речь идет лишь о детализации уже закрепленного объекта правоотношений. Являясь разновидностью результатов интеллектуальной деятельности, указанные объекты правоотношений будут иметь свои особенности, которые отразятся на гражданском обороте:

– такие объекты создаются не человеком, а нейросетью, но при участии человека;

– элемент творчества проявляется в синхронизации множества объектов в единый результат под воздействием внедренных в нейросеть алгоритмов;

– создатель нейросети не имеет притязаний на РИД;

– созданные объекты должны иметь меньшую оценку по сравнению с традиционными РИД.

Представляется, что перечисленные особенности придают РИД, созданным с применением ИИ, особый правовой режим, который и следует отразить в нормах ГК РФ. Установление нового правового режима и является решением существующих дискуссий. По нашему мнению, правовой режим должен учитывать отсутствие прав на такие РИД у создателя нейросети.

Список литературы

1. Вавилин Е. В. Искусственный интеллект как участник гражданских отношений: трансформация права // Вестник Томского государственного университета. Право. 2021. № 42.

2. Василевская Л. Ю. Цифровизация гражданского оборота: проблемы и тенденции // Российский юридический журнал. 2020. № 6(135). С. 105-117.

3. Габов А. В. Цифровой рубль центрального банка как объект гражданских прав // Актуальные проблемы российского права. 2021. Т. 16, № 4(125). С. 55–65.

4. Довлатова А. М. Фундаментальные начала гражданского права как основа практической деятельности правотворческих органов и субъектов // Евразийское Научное Объединение. 2020. № 10-5(68). С. 355-357.

5. Дулатова Н. В. Искусственный интеллект: понятие и правосубъектность // Частное право в эволюционирующем обществе: традиции и новации: сборник научных статей 2-й Всероссийской научной конференции, посвященной памяти д-ра юрид. наук, проф. В. Н. Сусликова / отв. редактор В. В. Богдан. 2020. С. 246-249.

6. Интервью А. И. Клименко о теории права в эпоху цифровизации. URL: https://youtu.be/EB06GKXB5eY

7. Калятин В. О. Определение субъекта прав на результаты интеллектуальной деятельности, созданные с использованием искусственного интеллекта // Право. Журнал Высшей школы экономики. 2022. № 4. С. 24-50.

8. Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дис. … д.-ра юрид. наук. М., 2018. 420 с.

9. Нейросети для генерации музыки. URL: https://dzen.ru/a/Y-JExb-HXE-1usxQ

10. Нейросеть за один вечер написала диплом за российского студента. URL: https://www.msk.kp.ru/daily/27460/4714947

11. Раянов Ф. М. Фундаментальные основы современной философии права // Юридическая наука: история и современность. 2016. № 8. С. 184-188.

12. Толковый словарь С. И. Ожегова онлайн. URL: https://gufo.me

13. Тумаков А. В., Петраков Н. А. Проблемы правовой охраны объектов, созданных с использованием технологий искусственного интеллекта // Цивилист. 2022. № 4. С. 16-28.

Е. В. Мартыненко,
доктор политических наук, профессор,
Российский университет дружбы народов
имени Патриса Лумумбы

ФРАНЦУЗСКАЯ МОДЕЛЬ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ: ОСНОВНЫЕ ТЕНДЕНЦИИ В ПРАВОВОЙ СФЕРЕ

Аннотация. В статье представлен обзор мер, которые принимаются во Франции для защиты сбора, обработки и хранения персональных данных. В частности, проанализированы трансформация Закона об информатике и гражданских свободах с 1978 года по настоящее время, а также деятельность Национальной комиссии по информатике и гражданским свободам, формирование ее приоритетов, находящихся в прямой зависимости от тенденций глобального киберпространства. Статья подготовлена в рамках инициативной НИР кафедры теории и истории журналистики РУДН № 050737-2-000 «Исследование медиасистем и медиаиндустрии России и мира: научно-образовательная компонента».

Ключевые слова: право, законодательство, киберугрозы, персональные данные, цифровые технологии, утечка данных, таргетированная реклама, Франция

FRENCH MODEL OF PERSONAL DATA PROTECTION: MAIN TRENDS IN THE LEGAL FIELD

Abstract. This article is an overview of the measures taken in France to protect the collection, processing and storage of personal data. In particular, the transformation

of the Law on Computer Science and Civil Liberties from 1978 to the present day is analyzed, as well as the activities of the National Commission on Computer Science and Civil Liberties, the formation of its priorities depending on trends in global cyberspace.

Keywords: law, legislation, cyber threats, personal data, digital technologies, data leakage, targeted advertising, France

Введение. Развитие современных технологий с каждым годом все более актуализирует вопрос защиты персональных данных: возможности бесконтактной оплаты, использование социальных сетей, подключение к сетям Wi-Fi в связи с расширением охвата связью во многих странах – все эти достижения, с одной стороны, упрощают жизнь человека, с другой – делают его конфиденциальную информацию более уязвимой. Так, по данным агентства «Интерфакс», с 2020 года в мире наблюдается резкий скачок числа киберпреступлений и связан он с пандемией коронавируса, из-за которой человечество стало более активным в онлайн-пространстве [3].

Если приводить в пример конкретные цифры, по данным IT-компании Positive Technologies, 2022 год стал годом массовой утечки персональных данных: общее количество киберпреступлений в мире выросло более чем на 20 %, и в данном случае речь идет лишь об успешных, то есть достигших цели (принесших негативные последствия конкретным лицам или компаниям) инцидентах: более 700 атак за каждый квартал вместо показателя 2021 года – 604 в среднем за квартал. При этом в атаках на организации добиться цели злоумышленникам удалось в 47 % случаев, а что касается частных лиц, их данные утекли в Сеть в 64 % случаев [1].

Подобные тенденции придают значимости исследованиям, связанным с защитой персональных данных в Сети. Обращаясь к истории защиты персональных данных и современным тенденциям в этой сфере на сегодняшний день, необходимо привести в пример Францию – страну, которая одной из первых стала рассматривать развитие информационных технологий как возможную угрозу неприкосновенности личной информации граждан.

Основная часть

Говоря о становлении термина Data Privacy, принято выделять два государства, повлиявших на его создание: Германию, где появился первый национальный закон о персональных данных в 1977 году, и Францию, где буквально через год, в 1978 году, приняли Закон об информатике и гражданских свободах.

Данный закон был принят после «скандала Сафари»: в начале 1970-х годов власти Франции разработали проект SAFARI, который должен был создать с помощью вычислительных технологий некий единый список, содержащий номера социального страхования всех граждан страны. Таким образом, реестр давал бы возможность идентифицировать любого жителя Франции при каждом его обращении в какие-либо ведомства и организации. Однако информация об этой задумке дошла до редакции газеты Le Monde, которая раскрыла подробности проекта широкой общественности – в статье под названием «Сафари, или Охота на французов». Материал оказался резонансным, общество стало требовать отменить проект, но при этом принять закон, защищающий личные данные граждан.

Публикации Le Monde привлекли внимание к проблеме отсутствия должной защиты персональной информации не только среди жителей Франции, но и среди простых граждан и экспертов в сфере права за рубежом. Данную тему начали обсуждать в международных организациях, и результатом этих обсуждений стал первый в истории международный договор в сфере защиты данных – Конвенция о защите физических лиц при автоматизированной обработке персональных данных.

Рассматривая французскую модель законодательства в области защиты данных, стоит отметить, что Франция совершенствует область защиты данных год от года – ее опыт перенимают многие другие государства. Например, именно власти Франции стали заявлять, что законы о защите информации нуждаются в реформировании с течением времени, в связи с появлением новых технологий, моральным устареванием уже существующих инструментов коммуникации и надзора за ней, а также политическими, экономическими и социальными факторами, одним из которых стало членство Франции в Европейском союзе. Таким образом, Закон 1978 года пережил ряд поправок. наиболее важные изменения коснулись его в 2004 году, когда Франция как государство – член ЕС стала учитывать Европейскую директиву о защите данных, и в 2016 году, когда был принят Закон «О цифровой республике», адаптирующий существующее законодательство под глобальный тренд цифровизации. Данный закон повлиял на французский Кодекс об интеллектуальной собственности, поскольку предусматривал исключение из категории авторского права сбора информации из объема больших текстовых/цифровых данных в целях анализа общественностью и учеными.

Интересен тот факт, что Франция, будучи страной Евросоюза, не отказалась от своей архитектуры законов, а лишь постаралась интегрировать их в отношении норм, провозглашенных в ЕС. Примером такой позиции может стать вступление в силу на территории ЕС в 2018 году европейского регламента по защите персональных данных, больше известного как GDPR (General Data Protection Regulation). Согласно регламенту, персональными данными считается любая информация, которая относится к субъекту данных (так называют любое идентифицированное или идентифицируемое физическое лицо), то есть та информация, с помощью которой можно определить ее владельца. К данной категории информации относятся ФИО, сведения о местоположении физического лица (геолокация), а также другие онлайн-идентификаторы вплоть до IP-адресов. Регламент носит экстерриториальный принцип по уровню охвата: иными словами, его положения могут быть применены ко всем организациям, которые обрабатывают персональные данные физических лиц из ЕС, даже если эти организации находятся за пределами Евросоюза.

Кроме этого, регламент устанавливает несколько типов данных, которые считаются особыми: это генетические и биометрические данные (в случае, если их используют с целью идентификации), данные о расовой и этнической принадлежности гражданина, ориентации, политических и религиозных убеждениях, а также статус членства в профсоюзах, поскольку все эти факторы можно использовать во вред человеку, а также с целью маркетинга и таргетированной рекламы.

Принятие регламента означало для Франции необходимость пересмотра Закона 1978 года, так как ряд его положений противоречил пунктам Регламента европейского образца, либо в какой-то степени отличался от них. Так, Правительство Франции внесло ряд поправок в Закон в виде дополнений к Регламенту.

Согласно этим поправкам, возраст предоставления согласия на обработку данных во Франции начинается с 16 лет. Во-вторых, в государстве существует специальный регистр Bloctel, где каждое физическое лицо может зарегистрироваться, и регистрация в списке означает желание отказаться от каких-либо рекламных звонков, писем и сообщений. Срок действия отказа – три года, однако его можно продлевать.

Также французское законодательство отдельно рассматривает персональные данные умерших лиц – считается, что изучение и обработку таких данных можно проводить, если человек при жизни не выразил отказ от данных шагов.

Не менее интересна и сфера деловых отношений, которую тоже затрагивают поправки Закона 1978 года. Работодатель во Франции имеет право отслеживать геолокацию транспортных средств, которые водят сотрудники в рабочее время (например, если речь идет о водителях такси, курьерах и т. п.), записывать телефонные разговоры в сферах обучения или обслуживания с целью их анализа для дальнейшей оценки эффективности, а также изучать рабочую электронную почту сотрудников (за исключением писем, которые сотрудник помечает как «Личное»).

Францию от других государств ЕС отличает наличие собственной комиссии по защите конфиденциальности данных. Ее название – Национальная комиссия по информатике и гражданским свободам (CNIL) [4]. Данная комиссия является независимым административным регулирующим органом. Его задача – обеспечивать исполнение закона о конфиденциальности данных при их сборе, хранении и использовании. Эта комиссия появилась, как и главный закон о защите информации Франции, в 1978 году, и даже после введения единых нормативов на территории Евросоюза, власти страны решили не отказываться от данной организации.

Национальная комиссия выполняет целый ряд функций: регистрирует установку информационных систем, которые обрабатывают персональные данные на территории страны, также следит за исполнением законов в данной области, проводит расследования в случае неприменения норм местного законодательства и выносит предупреждения или санкции организациям, нарушающим их. Более того, комиссия имеет право принимать различные рекомендации и кодексы в сфере защиты персональных данных.

В структуре комиссии – 17 представителей различных правительственных организации Франции. Так, к примеру, четверо представителей комиссии должны быть членами парламента.

Авторитет комиссии настолько высок, что с 2018 года она обладает правом формировать собственный черный список организаций, нарушающих закон в сфере защиты персональных данных. При этом комиссия изменила свою методичку для организаций в связи с нормами GDPR, внеся изменения в руководство по изучению файлов cookie и других инструментов отслеживания, а также в руководство по оценке воздействия на защиту данных.

Работа комиссии меняется каждый год, в соответствии с изменениями в цифровой среде и медиапространстве Евросоюза. В 2021 году комиссия объявила о запуске «песочницы». Так в сфере IT называется специальная система по поиску вредоносных программ, причем ее виртуальные машины изолированы от реальной коммуникационной инфраструктуры комиссии. Система помогает найти уязвимые места, выявить подозрительные коды, противостоящие атакам на программное обеспечение комиссии, поскольку она занимается большими данными, касающимися всех граждан Франции. То есть комиссия не только следит за безопасностью персональных данных в других системах, но и стремится защитить свою информацию, потому что является главным регулятором Big Data в стране.

Что касается санкций, которые имеет право вводить комиссия в отношении организаций, работающих с персональными данными граждан Франции, в частности, они могут быть введены за несоблюдение правил по обработке данных, отказ от сотрудничества с надзорными органами Франции, нарушение принципов безопасности данных, несоблюдение обязательств по ограничению срока хранения данных пользователей и за несоблюдение требований по оформлению cookie-файлов. К последнему пункту относятся отсутствие информации о сборе cookie-файлов сайтом и отсутствие запроса на согласие на cookie.

Все эти нововведения способствовали появлению новых терминов и должностей, связанных с защитой персональных данных. Во многом эти термины соотносятся с положениями GDPR. Например, во Франции появились контроллеры данных и процессоры данных. Контроллеры – это компании либо организации, собирающие данные пользователей. Процессорами считаются компании, которые эти данные обрабатывают. К слову, примечательно, что в Законе 1978 года определения данных терминов отсутствуют, поскольку Франция посчитала лишним дублировать их, ведь они и так содержатся в Регламенте.

При этом комиссия более чем щепетильна во всем, что касается трендов цифровой среды Франции. Летом 2023 года эксперты организации приступили к исследованию, изучающему уровень использования мобильных технологий в стране. Оно показало, что 87% населения Франции в возрасте от 12 лет владеют смартфонами, и для них это – наиболее предпочтительное устройство, чтобы подключиться к сети Интернет. «Данная тенденция наглядно демонстрирует важность мобильных телефонов и планшетов в повседневной цифровой жизни французов», – указано в отчете. При этом столь массовое использование смартфонов означает и массовое использование мобильных приложений, которые, в свою очередь, создают весьма серьезные проблемы с точки зрения защиты конфиденциальности пользователей. Поэтому тема мобильных приложений была включена в список приоритетов работы комиссии [5].

Несмотря на то, что большое количество мобильных приложений предлагает те же услуги, что и их сайты-эквиваленты, техническая среда, в которой работают веб-сайты и мобильные приложения, разные. Основное отличие заключается в том, что использование мобильных приложений позволяет обрабатывать больше объемов персональных данных – к примеру, мобильное приложение может получить доступ к контактной книге физического лица.

В рамках исследования комиссия провела консультации с рядом игроков в сфере мобильных приложений, а именно с создателями и разработчиками приложений, поставщиками комплектов для разработки ПО и ОС для мобильных приложений, а также представителями магазинов приложений. Итогом всех этих консультаций стал проект рекомендаций, который вынесен во Франции на общественное обсуждение до 8 октября 2023 года. Данный проект предполагает, что разрешения на доступ к таким конфиденциальным ресурсам, как геолокация, список контактов, камера мобильного телефона, заметки и файлы, должны разрабатываться и использоваться таким образом, чтобы в первую очередь защищать права людей. А для этого приложения должны предоставлять четкую информацию о том, необходимо ли согласие на доступ приложения к данным для корректного функционирования приложения, выполнения каких-либо вспомогательных функций, а также поможет ли согласие финансировать приложение без оплаты, например, с помощью таргетированной рекламы (таким образом, пользователь будет знать, идут ли его персональные данные в основу для рекламы).

Эксперты комиссии рекомендуют поставщикам ОС для мобильных приложений также внедрить целый ряд передовых методов для содействия созданию «среды с уважением к защите персональных данных» – речь идет о повышении качества и надежности информации, доступной пользователям, и предоставлении им большего контроля над обработкой данных, которую осуществляют мобильные приложения.

Еще один приоритет текущего года для комиссии в сфере защиты персональных данных – это стремительное развитие телемедицины. Франция призывает обращать внимание на эту сферу здравоохранения, ведь, с одной стороны, у телемедицины множество преимуществ – с помощью дистанционных консультаций врач может наблюдать хронических больных, становится реальным своевременное оказание медицинской помощи лицам, находящимся далеко от медицинских учреждений (например, в деревнях в горной местности), также более опытный врач может консультировать посредством телемедицинской консультации молодых коллег. Однако, с другой стороны, телемедицина – это сбор данных о пациенте, которые могут подвергнуться кибератаке. Учитывая данную опасность, в 2023 году комиссия заявила о сопровождении восьми проектов в области цифрового здравоохранения и секторе образовательных технологий. Поддержка заключалась в регулярных юридических и технических консультациях для клиник и университетов, благодаря которым те могли усилить защиту данных своих пациентов или учащихся.

Третьим приоритетом для комиссии стали изучение и мониторинг инновационных методов, используемых для разработки и эксплуатации инструментов искусственного интеллекта. Комиссия наблюдает за прозрачностью обработки данных, которые станут основой для деятельности ИИ, на территории Франции, а также за защитой данных, которые передают пользователи при работе с ИИ: начиная от банального сбора информации о пользователе и заканчивая возможностью их повторного использования и обработки для построения алгоритмов машинного обучения. Комиссия также анализирует последствия работы с ИИ –

например, как генеративный ИИ создает контент на основе информации, полученной от пользователей. Важным аспектом в данном случае является риск формирования какой-либо предвзятости или дискриминации, проводимой при подаче данных, а также риск нарушения безопасности пользователей – утечки их персональной информации.

Стоит подчеркнуть, что комиссия не только разрабатывает рекомендации и выносит их на обсуждение. В Европейском суде организация известна своими громкими делами, начатыми из-за нарушений сбора, обработки и хранения данных граждан Франции. Так, в июне 2023 года комиссия наложила штраф в размере 40 миллионов евро на компанию, специализирующуюся на онлайн-рекламе, – CRITEO. Причиной для штрафа стал тот факт, что компания не смогла подтвердить наличие согласий на обработку данных со стороны лиц, информацию о которых она обрабатывала с целью формирования таргетированной рекламы. При этом обработка касалась большого количества людей – CRITEO обладала данными, относящимися примерно к 370 млн идентификаторов по всему Европейскому союзу. Несмотря на то, что компания собирала информацию о потребительских привычках пользователей и не хранила их имена, комиссия сочла, что данные о привычках каждого пользователя были настолько точными, что в некоторых случаях идентификация людей не составила бы труда: например, регулярная отметка одних и тех же геолокаций, совершение одних и тех же покупок, заказов и т. п.

Политика конфиденциальности компании не была полной, поскольку она не включала все предполагаемые цели обработки. Кроме того, некоторые цели были выражены расплывчато и широко, что не позволяло пользователю точно понять, какие персональные данные используются и для каких целей. Когда человек воспользовался своим правом отозвать согласие или удалить свои данные, процесс, реализованный компанией, только остановил показ персонализированной рекламы пользователю. Однако компания не удалила идентификатор, присвоенный человеку, и не стерла навигационные события, связанные с этим идентификатором. Наконец, комиссия посчитала, что обработка столь больших объемов данных позволила CRITEO значительно увеличить свой финансовый доход.

Другим не менее громким делом этого года стало инфоцыганство. Комиссия оштрафовала на 150 тысяч евро за несоблюдение правил французского законодательства и GDPR портал KG COM, который собирал «чрезмерные и чувствительные» конфиденциальные данные без предварительного и явного согласия пользователей, а также в недостаточной степени обеспечивал безопасность данных. Сайт продавал предсказания будущего, которые передавались либо в чате, либо с помощью телефонного разговора. В 2020 году во французских СМИ появилась информация, что сайт допустил утечку данных, и комиссия решила заняться его мониторингом.

«В ходе расследования комиссия заметила несколько нарушений, касающихся, в частности, систематической записи телефонных звонков, сбора данных о здоровье и информации, касающейся ориентации, а также банковских данных физических лиц без их согласия», – указано в отчете о расследовании.

Дело об инфоцыганстве привлекло внимание правоохранителей на территории всего ЕС в связи с тем, что комиссия в ходе расследования сотрудничала с коллегами из Бельгии, Люксембурга, Италии, Испании, Португалии и Болгарии, поскольку лица из этих стран также были клиентами сайта.

Самым громким делом комиссии, однако, стали разбирательства с Google. По мнению экспертов организации, использование американского программного обеспечения создало риск незаконного доступа к персональным данным пользователей Франции со стороны властей США. Комиссия сочла, что сервис Google Analytics несет угрозу конфиденциальности пользовательских данных, поскольку не дает гарантий, что они не попадут властям Штатов [2]. Кроме этого, в 2021 году комиссия отметила, что Google LLC и Google Ireland Limited нарушают европейские требования, распространяющиеся на cookie-файлы, потому как вопрос о согласии или отказе от них не выглядит явным. В результате комиссия наложила на компанию штраф в размере 150 миллионов евро. А невыполнение требований в дальнейшем подвергло Google уплате дополнительных штрафов в сумме 100 тысяч евро за каждый день просрочки.

Заключение. Резюмируя все эти тенденции, можно прийти к выводу, что Франция продолжает уделять повышенное внимание защите персональных данных своих граждан, в связи с чем делает акценты на регулярном реформировании законодательства в данной сфере, проработке эффективной интеграции местных надзорных органов с GDPR в рамках Евросоюза, а также в рамках Национальной комиссии каждый год формирует список приоритетов возможных рисков для защиты персональных данных в стране. Важным моментом является и прозрачность всех мер, предпринимаемых во Франции для обеспечения конфиденциальности данных: комиссия регулярно публикует отчеты о своей деятельности, все нормативы перед принятием выносятся на общественное обсуждение и подкрепляются аналитическими исследованиями, консультантами которых выступают практики цифровой отрасли. Французская модель охраны данных, безусловно, является интересной для изучения в условиях роста киберугроз по всему миру, поскольку надежность сбора, обработки и хранения информации о пользователях способствует формированию устойчивой цифровой экономики и укрепляет информационную безопасность страны.

Список литературы

1. Актуальные киберугрозы: итоги 2022 года. URL: https://www.ptsecurity.com
2. Во Франции предложили способ защиты данных пользователей в Интернете. URL: https://rossaprimavera.ru
3. Мошенничество в сети: итоги 2022 года. URL: https://spark-interfax.ru
4. Commission nationale de l'informatique et des libertés. URL: https://www.cnil.fr
5. CNIL. Mobile applications: CNIL launches a public consultation on its draft recommendation. URL: https://www.cnil.fr

С. А. Минич,
младший научный сотрудник,
Национальный центр законодательства
и правовых исследований Республики Беларусь

ЗАКОНОДАТЕЛЬСТВО С ОГРАНИЧЕННЫМ СРОКОМ ДЕЙСТВИЯ – ЭФФЕКТИВНЫЙ ИНСТРУМЕНТ АКТУАЛИЗАЦИИ НОРМАТИВНОГО МАССИВА В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Аннотация. Активное развитие цифровых технологий в условиях современности вызывает непрерывное обновление законодательства, ставя под сомнение его стабильность, соответствие запросам сегодняшнего дня. На фоне цифровизации, открывающей огромные преимущества для всех сфер жизнедеятельности, наблюдается определенное отставание нормативных правовых актов от темпов технологического прогресса, что требует своевременного обновления и оптимизации правовой базы, быстрого и недифференцированного устранения устаревших, неактуальных норм. Процесс широкомасштабного обновления законодательства, необходимость его непрерывного пересмотра предполагает использование эффективных правовых инструментов дерегулирования, среди которых отдельного внимания заслуживает законодательство с ограниченным сроком регуляторного действия. В статье рассмотрены сущностные характеристики, преимущества и отличительные особенности данного инструмента, проанализирован опыт ряда стран по его успешному использованию.

Ключевые слова: цифровизация, право, дерегулирование, закатное законодательство, актуализация нормативного массива

LEGISLATION WITH A LIMITED VALIDITY PERIOD IS AN EFFECTIVE TOOL FOR UPDATING THE REGULATORY ARRAY IN THE CONDITIONS OF DIGITALIZATION

Abstract. The active development of digital technologies in modern conditions causes continuous novelization of legislation, calling into question its stability, compliance with the demands of today. Against the background of digitalization, which opens up huge advantages for all spheres of life, there is a certain lag of regulatory legal acts from the pace of technological progress, which requires timely updating and optimization of the legal framework, rapid and undifferentiated elimination of outdated, irrelevant regulations. The process of large-scale updating of legislation, the need for its continuous revision involves the use of effective legal instruments of deregulation, among which legislation with a limited period of regulatory action deserves special attention. The article considers the essential characteristics, advantages and distinctive features of this tool, analyzes the experience of a number of countries in its successful use.

Keywords: digitalization, law, deregulation, sunset legislation, updating of the regulatory array

Введение. В эпоху цифровых преобразований, прорывных технологических достижений возникает необходимость перенастройки правового регулирования общественных отношений, исключая его избыточный характер, сокращая обременительные и устаревшие нормы, способствуя созданию благоприятных условий для внедрения цифровых новшеств, привлечения инвестиций и поддержания устойчивой конкурентоспособности страны в цифровой сфере. Цифровизация занимает одно из приоритетных мест в современной государственной политике многих стран, представляя собой закономерный эволюционный процесс преобразования всех сфер жизнедеятельности общества, направленный на последовательный переход в сторону гибких, качественно иных форм принятия решений, требующих учитывать особенности новой цифровой реальности. Развитие цифровых технологий привело к появлению большого количества новых норм в уже сложившихся отраслях и институтах права и одновременно выявило наличие значительного массива неактуальных, неработающих регуляций в действующем законодательстве, создающих определенные барьеры для развития цифровых технологий, сдерживающих внедрение инноваций и тормозящих социально-экономическое развитие страны в целом. Возникшие трудности привели к зарегулированности общественных отношений в той или иной сфере и потребовали активного поиска действенных правовых инструментов быстрого устранения законодательных «завалов» и оптимизации всего нормативного массива, адаптации регулирования к изменяющимся социальным и технологическим обстоятельствам. Значительным потенциалом недифференцированного сокращения устаревших, противоречивых правовых норм обладает законодательство с ограниченным сроком регуляторного действия, позволяющее заранее запрограммировать исчерпание регуляторного потенциала действия отдельных нормативных правовых актов по завершении конкретного периода времени, установленного в положениях о прекращении действия. Целесообразность рассмотрения сущностной составляющей данного правового инструмента дерегулирования общественных отношений обусловлена наращиванием темпов цифровой трансформации и ускорением процессов выработки новых правовых норм.

Основная часть. В зарубежной правовой доктрине законодательство с ограниченным сроком действия получило название «закатное законодательство», или «законодательство о закате». Среди немногочисленных дефиниций наиболее лаконичная, на наш взгляд, представлена М. В. Дегтяревым, который, раскрывая концепт самозавершающегося нормативного правового акта, резюмирует, что под ним следует понимать «нормативный правовой акт с изначально запрограммированным прекращением (по исчерпании предписанного регуляторного потенциала) действия, включающий правовые положения, которые предусматривают автоматическое прекращение действия регулирования по исчерпании их телеологической (целевой) нагрузки (потенциала) к тому времени, когда это по факту произойдет, либо в определенную дату (по истечении определенного периода времени, куда уже расчетно закладывается исчерпание регуляторного потенциала), если уполномоченный законодательный орган специально не примет положительных мер для продления действия этого нормативного акта [1, с. 165].

Ключевой особенностью «закатного законодательства» выступает наличие в нормативных правовых актах положения о прекращении действия (положения «о закате»), где заранее определена дата истечения срока его юридической силы, на который он был принят [2]. Можно сказать, что жизненный цикл такого нормативного акта предварительно искусственно определен законодателем, т. е. предусмотрен еще на этапе его разработки. Прекращение действия всего акта или его отдельного структурного элемента происходит одномоментно, он утрачивает свою нормативную силу автоматически, что свидетельствует об исчерпании его регуляторного потенциала. Такой подход позволяет поддерживать правовой массив в актуальном состоянии, своевременно обновлять нормативную базу с учетом ускоренного ритма развития цифровых технологий, демонстрирует мобильный характер законодательства, его открытость для современных инновационных разработок и желаемым цифровым преобразованиям сегодня и в будущем.

Если обратиться к истокам зарождения закатного законодательства, то корни положений «о закате» уходят в римское право. Правило Ad tempus concessa post tempus censetur denegata в переводе с латинского звучит как «то, что разрешено на определенный период, будет отклонено после истечения срока». Данный принцип был также отражен в Кодексе Юстиниана [3].

В зарубежных странах, активно использующих закатное законодательство (Германия, Австралия, Нидерланды, Израиль, США и др.), постепенно сформировалась установка, что устаревание законодательства может стать платой за сохранение правил, которые действуют дольше общественных отношений, которые ими регулируются. Так, к примеру, немецко-американский юрист Фрэнсис Либер в свое время акцентировал внимание на следующем обстоятельстве: «Все, что содержится в кодексе, который не соответствует духу общества, должно упасть на землю» [4. С. 14].

В США положения «о закате» появились еще в XVIII веке. В 1789 г. Томас Джефферсон в своем письме Джеймсу Мэдисону отмечал: «Ни одно общество не может создать вечную конституцию или даже вечный закон. Земля всегда принадлежит живущему поколению. <...> Таким образом, срок действия каждой конституции и каждого закона, естественно, истекает по истечении 34 лет. Если это будет продолжаться дольше, то это будет акт силы, а не права» [5]. При этом Томас Джефферсон обращал внимание на важную особенность в данном процессе, отмечая, что законодательные акты не обязательно должны прекращать свое действие по истечении определенного периода. К примеру, некоторые законы естественным образом отстают от эволюции общества и технологий, однако другие переживают разные поколения или могут быть обновлены. Высказанная таким образом идея впоследствии получила свое отражение в ряде нормативных правовых актов США. Соответственно, одной из положительных сторон «закатного законодательства» выступала его способность создавать так называемые совещательные преимущества, благодаря которым открывалась возможность внести необходимые изменения в регулирование, а также блокировать продолжение неэффективных регуляторных решений. Среди очевидных неоспоримых плюсов также следует указать, что отмена постоянного законодательства являлась более трудоемкой

и дорогостоящей процедурой, в сравнении с использованием самозавершающихся нормативных правовых актов.

В США на уровне штата первые законодательные акты, включающие положения «о закате», были приняты в 1976 г. (штат Колорадо). Далее в период с 1976 по 1982 г. законодатели 36 штатов приняли нормативные правовые акты, содержащие положения «о закате». По состоянию на 2014 г. только в трех штатах никогда не принимались подобные законы (Айова, Массачусетс, Северная Дакота) [6]. Время же между вступлением в силу (или продлением) и следующей датой «заката» варьировалось от штата к штату, но обычно составляло от четырех до двенадцати лет. В США также были учреждены специальные консультативные комиссии для периодической оценки и пересмотра существующих самозавершающихся нормативных правовых актов; проведения слушаний по вопросам, регулируемым такими актами; принятия решения об их отмене или возобновлении. Сохранившаяся Консультативная комиссия Техасского заката – один из самых известных тому примеров. Несмотря на то, что развитие законодательства о закате на тот момент не было обусловлено процессами цифровизации и такие акты принимались в первую очередь в целях контроля и ограничения полномочий ведомств (агентств), отслеживания государственных расходов и повышения подотчетности органов власти, а позднее – в качестве инструмента для оценки рисков и последствий новой политики регулирования, однако их потенциал по оптимизации правового массива и возможность максимально быстро адаптировать регулирование к изменяющимся условиям приобретает особую актуальность в период интенсивного погружения в цифровую реальность.

В Германии и Нидерландах положения о прекращении действия применялись в целях снижения риска чрезмерного правового регулирования и проведения мягких реформ дерегулирования для ограничения срока действия законов и иных нормативных правовых актов, исчерпавших свой регуляторный ресурс, а также для проведения их последующей оценки (ex post), от которой зависело их продление или прекращение действия.

В Нидерландах аргументы в пользу «закатного законодательства» впервые были представлены в научных работах известных юристов в 1970-х годах. К примеру, Роэл ин’т Вельд в своих трудах отмечал, что, поскольку проблемы меняются с течением времени (часто даже до того, как они будут решены), таким же должно быть и регулирование, чтобы избежать устаревания [7. С. 65]. В 1980-х годах группа голландских исследователей рассмотрела в положениях «о закате» (horizon-bepalingen) инструмент, позволяющий отражать динамику законодательства и прекращать действие тех нормативных правовых актов, которые не достигали целей, ради которых они были приняты, или когда регулирование оказывалось неэффективным для их достижения [7. С. 139]. Несмотря на активное и широкое обсуждение данного вопроса, а также проведенную в 1980-х годах реформу регулирования, направленную на сокращение и недопущение принятия чрезмерного количества нормативных правовых актов, положения о прекращении действия в законодательстве Нидерландов появились лишь в 1990-е годы, а акты, их содержащие, стали рассматриваться как эффективный механизм

актуализации нормативной базы, повышающий качество правового регулирования в условиях быстрого технологического развития и цифровой глобализации. Так, в 1992 г. был принят первый временный закон, направленный на стимулирование и финансирование социального обновления (sociale vernieuwing) в условиях экономического кризиса (Tijdelijke bepalingen ter stimulering en bekostiging van sociale vernieuwing). Этот закон включал положение о прекращении действия и был представлен как гибкий и простой инструмент в контексте дерегулирования. Отметим, что в законодательстве Нидерландов срок действия законодательных актов, включающих положения о закате, колеблется между одним и шестью годами.

В Германии, перед тем как принять решение о целесообразности «закатного законодательства», долгое время изучалась причинно-следственная связь между использованием такого вида временного законодательства и снижением излишнего регуляторного давления, а также последующим стимулированием инноваций. В результате проведенного научного поиска немецкие ученые пришли к выводу, что принятие самозавершающихся нормативных правовых актов в условиях активно развивающихся рынков телекоммуникационных услуг, информационных технологий позволит избежать угрозы их «свободному и инновационному развитию» [7. С. 37]. Таким образом, в Германии было предложено рассматривать использование положений о прекращении действия более широко, а именно в качестве способа обеспечения устранения ненужного бремени регулирования, тем самым создавая благоприятные условия для привлечения инвестиций и внедрения инноваций. Начиная с 2004 г. в Германии многие земли использовали «закатное законодательство». Согласно эмпирическому исследованию, проведенному Фондом Бертельсманна в 2010 г., было выявлено, что количество нормативных правовых актов, включающих положения о прекращении действия, варьировалось от 6% (в Нижней Саксонии) и более чем 60 % (в Гессене, Северном Рейне-Вестфалии, Саарe) [8].

Важной особенностью «закатного законодательства» Германии была строгая установка о том, что законы, содержащие положение «о закате», в принципе не могут быть изменены до даты истечения их срока действия. Любые изменения или пересмотры должны приниматься только в особых случаях и с учетом общественных интересов. Такой подход демонстрирует, что самозавершающиеся законодательные акты включают определенные гарантии, обеспечивающие непрерывность их действия в течение определенного времени, поэтому в проведении какой-либо корректировки или прекращении их действия до установленного срока должно быть категорически отказано [7. С. 177]. Учитывая, что в Германии срок действия нормативных актов, определенный в положениях о прекращении действия, обычно составляет пять лет, соответственно гражданам предоставляется четкая правовая определенность в отношении неизменности их прав и обязанностей в течение всего этого временного периода.

Примером страны, где на сегодняшний день «закатное законодательство» используется наиболее часто, выступает Израиль. Например, с 2000 по 2015 г. Кнессет принял 281 временный закон. Доля временных законов в 2013 г. достигла своего пика, составив 15,41% от всех принятых законов [9. С. 32]. Кнессет использовал временное законодательство в качестве средства решения проблем регулирования

в широком спектре областей: меры по борьбе с терроризмом, клонирование человека, иммиграция, налоговое законодательство, борьба с экономическим кризисом и др. Среди целей, лежащих в основе самозавершающихся нормативных правовых актов, принимаемых в Израиле, выступают временные решения какой-либо неотложной проблемы или урегулирование кризисной ситуации. Продолжительность действия временных законов, содержащих положение «о закате», варьируется от 3,5 месяцев до 5 лет.

В Австралии в 2003 г. был принят Закон о законодательных актах (Legislative Instruments Act 2003, LIA), целями которого обозначены: отмена устаревших законодательных актов или их отдельных положений (через 10 лет после принятия); создание механизмов для обеспечения периодического пересмотра законодательных актов и их отмены, если в их сохранении более нет необходимости.

В постсоветских странах законодательство с ограниченным сроком действия не получило своего широкого распространения и применяется в основном относительно подзаконных нормативных правовых актов, имеющих временный характер. При этом данные акты не рассматриваются в качестве эффективного правового механизма дерегулирования. Их принятие обусловлено, как правило, иными целями, нежели своевременная актуализация и оптимизация нормативного массива, позволяющая закону идти в ногу с ускорением, действовать на опережение, защищая возможности, открываемые развитием цифровых технологий на благо человека и общества.

Заключение. Подводя итог вышесказанному, следует отметить, что в эпоху цифровых преобразований стремление бороться с зарегулированностью, обусловленной устаревшим и излишним законодательством, которое больше не достигает своих первоначальных целей и не соответствует динамике развития современного общества путем недифференцированного сокращения нормативного массива, приобретает особую значимость. Эффективное нормативно-правовое регулирование любого социального и технологического явления подразумевает понимание его сущностных характеристик и быстрое реагирование на многовекторные изменения, которые им обусловлены. Целесообразность использования механизма правового дерегулирования, основанного на принятии нормативных правовых актов с ограниченным сроком действия, в условиях глобальных цифровых трансформаций и турбуленций является очевидным. Закатное законодательство – пример, когда регулятивные меры являются не только легкими, но и разумными, мобильными, менее затратными, открытыми для инновационно-технологических достижений. Обладая свойствами опережающего отражения действительности, данный вид временного законодательства позволяет в более сжатые сроки адаптировать регулирование к изменяющимся технологическим обстоятельствам, заранее определив «жизненный цикл» нормативных правовых актов, избегая таким образом избыточного регулирования в той или иной сфере общественных отношений. Анализ зарубежного опыта продемонстрировал, что активное использование законодательства с ограниченным сроком действия вызвано объективной потребностью актуализации нормативной правовой базы, имеющей с течением времени тенденцию к росту и постепенному отдалению от текущей реальности, что значительно снижает качество регулирования.

Список литературы

1. Дегтярев М. В. Концепт самозавершающихся нормативных правовых актов в правовой доктрине и практике США // Право и государство: теория и практика. 2021. № 6(198). С. 164-167.

2. Дегтярев М. В. Новейшие регуляторные технологии и инструменты: Регуляторные эксперименты, песочницы, гильотины, экосистемы, платформы / под ред. д. ю. н., проф. И. В. Понкина / МГЮА. М.: Буки Веди, 2022. 424 с.

3. Codex Iustinianus. Berolini: apud Weidmannos. URL: https://archive.org

4. Robert Luce A. M. Legislative Principles: The History and Theory of Lawmaking by Representative Government. Boston: Houghton Mifflin Company, 1930. 667 p.

5. Jefferson T. Letter to James Madison. URL: http://www.thefederalistpapers.org

6. Baugus B., Bose F. Sunset Legislation in the States: Balancing the Legislature and the Executive // Mercatus Research, Mercatus Center at George Mason University, Arlington, VA. URL: https://www.mercatus.org

7. Ranchordás S. H. Sunset clauses and experimental legislation: Blessing or curse for innovation. Koninklijke Wöhrmann B.V., Estlandsestraat 1, Zutphen, the Netherlands, 2014. 369 p.

8. Jantz B., Veit S. Sunset Legislation and Better Regulation: Empirical Evidence from Four Countries. URL: https://www.researchgate.net

9. Ittai Bar-Siman-Tov Temporary Legislation, Better Regulation and Experimentalist Governance : An Empirical Study // Regulation & Governance. 2018. Vol. 12, № 2. Pp. 192-219.

Е. А. Останина,
кандидат юридических наук, доцент,
Челябинский государственный университет

ОСОБЕННОСТИ ОСУЩЕСТВЛЕНИЯ И ЗАЩИТЫ ИСКЛЮЧИТЕЛЬНЫХ ПРАВ В СЕТИ ИНТЕРНЕТ: НЕКОТОРЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. Особенности творчества в сети Интернет заслуживают исследования. Во-первых, использование авторами нейросети вызывает вопрос о том, является ли «совместное творчество» автора и нейросети произведением, защищаемым нормами гражданского законодательства, и если да, то является ли автором созданного произведения гражданин, использовавший нейросеть, или программист, разработавший нейросеть (или же оба они являются соавторами). В статье аргументируется вывод о том, что нейросеть является одним из новых технических средств, использование которого не исключает творчества. Также рассматривается специфика отношений соавторства в сети Интернет и особенности цитирования в сети Интернет.

Ключевые слова: авторское право, соавторство, цитирование, творчество

FEATURES OF THE EXERCISE AND PROTECTION OF EXCLUSIVE RIGHTS ON THE INTERNET: SOME PROBLEMS OF LEGAL REGULATION

Abstract. The peculiarities of creativity on the Internet deserve research. Firstly, the use of a neural network by the authors raises the question of whether the "joint creativity" of the author and the neural network is a work protected by the norms of civil legislation, and if so, whether the author of the created work is a citizen who used a neural network or a programmer. The developer of the neural network (or both of them are co-authors). The report argues for the conclusion that the neural network is one of the new technical means, the use of which does not exclude creativity. The specifics of the relationship of co-authorship on the Internet and the features of citation on the Internet are also considered.

Keywords: copyright, co-authorship, citation, creativity

В феврале 2023 г. Бюро по авторским правам приняло решение о том, что иллюстрации, созданные художником с использованием нейросети Midjorney, не охраняются авторским правом. Таким образом, вопрос о том, как защищаются произведения, созданные с использованием нейросети, имеет уже не только теоретический, но и практический характер. В литературе уже высказано несколько точек зрения. Первая состоит в том, что разработчик программы должен получить исключительные права на созданный с использованием программы результат, вторая – в том, чтобы признать за искусственным интеллектом свойства квазисубъекта права, третья же точка зрения состоит в том, чтобы рассматривать результаты, созданные с использованием нейросети, наряду с классическими результатами творческой деятельности [1–3]. При этом исследователи отмечают, что решение должно создавать экономические стимулы и для лиц, разрабатывающих полезные для творчества программы, и для лиц, использующих эти программы в своем творчестве [4].

В основе своей эта проблема восходит к давней дискуссии о том, что такое творческий характер как признак произведения [5. С. 40–55]. Можно напомнить, что в ходе дискуссии о том, является ли объектом авторского права фотография или видеозапись, был сформулирован вывод о том, что использование технических средств само по себе не исключает творчества. Так, в п. 80 Постановления Пленума Верховного Суда РФ от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» отмечается, что «… творческий характер создания произведения не зависит от того, создано произведение автором собственноручно или с использованием технических средств. Вместе с тем результаты, созданные с помощью технических средств в отсутствие творческого характера деятельности человека (например, фото- и видеосъемка работающей в автоматическом режиме камерой видеонаблюдения, применяемой для фиксации административных правонарушений), объектами авторского права не являются». Таким образом, всякий раз, когда речь идет об использовании технических средств, нужно выяснить, какую еще деятельность осуществил тот, кто

претендует на авторство, была ли эта деятельность сугубо технической или же самостоятельной и связанной с индивидуальными особенностями автора. Если будет установлено, что гражданин осуществил целенаправленную деятельность по формированию запроса, поиску стиля, отбору вариантов, доработке результата, то и произведение, созданное с использованием нейросети, можно признать объектом авторского права.

Еще одной интересной проблемой является особенность регулирования новых отношений соавторства. Специфика отношений состоит в том, что соглашение о соавторстве между авторами отсутствует, соавторы в своем творчестве присоединяются к условиям пользования сайтом, что, по сути, является договором присоединения (ст. 428 ГК РФ). Созданные автором фрагменты складываются в общую картинку, при этом необходимо исключить коммерческое использование полученного общими усилиями творческого результата третьими лицами (Решение Суда по интеллектуальным правам от 07.04.2022 по делу № СИП-143/2021).

Заключение. Классические институты авторского права, такие как признаки произведения и понятие соавторства, несколько изменяются в период цифровизации. Варианты регулирования новых отношений могут быть предметом дискуссии.

Список литературы

1. Hacohen U. Y., Elkin-Koren N. Copyright Regenerated: Harnessing GenAI to Measure Originality and Copyright Scope // Harvard Journal of Law & Technology. 2024. Vol. 37, No. 2.

2. Murray, Michael D., Tools Do Not Create: Human Authorship in the Use of Generative Artificial Intelligence.URL: https://ssrn.com/abstract=4501543

3. Hayes, Carol Mullins, Generative Artificial Intelligence and Copyright: Both Sides of the Black Box. URL: https://ssrn.com/abstract=4517799

4. Frosio, Giancarlo, The Artificial Creatives: The Rise of Combinatorial Creativity from Dall-E to GPT-3 (February 7, 2023). Martha Garcia-Murillo, Ian MacInnes, and Andrea Renda (eds), Handbook of Artificial Intelligence at Work: Interconnections and Policy Implications (Edward Elgar, Forthcoming), Queen's University Belfast Law Research Paper. URL: https://ssrn.com/abstract=4350802

5. Ионас В. Я. Критерий творчества в авторском праве и судебной практике. М.: Юрид. лит., 1963. 137 с.

Д. Л. Пивненко,
соискатель,
Волгоградский государственный университет,
заместитель председателя,
Комитет государственной охраны объектов
культурного наследия Волгоградской области

ЧАСТНОПРАВОВЫЕ АСПЕКТЫ ВЕДЕНИЯ ЕДИНОГО ГОСУДАРСТВЕННОГО РЕЕСТРА ОБЪЕКТОВ КУЛЬТУРНОГО НАСЛЕДИЯ: ПРОБЛЕМА ТРАДИЦИОННЫХ И ЦИФРОВЫХ ТЕХНОЛОГИЙ ВИЗУАЛИЗАЦИИ ОБЪЕКТА

Аннотация. Цель исследования – выявление особенностей ведения Реестра объектов культурного наследия (памятников истории и культуры) народов Российской Федерации в части использования традиционных и возможности внедрения элементов цифровых технологий в части визуализации объектов. Выявлена проблема недостаточной разработанности нормативных правовых актов в части отражения определенного состава сведений в данном реестре и предъявляемых к ним требований. Обосновывается положение о закрытом характере перечня сведений, вносимых в указанный реестр в части их визуализации. Сделан вывод о необходимости корректировки законодательства, направленной на уточнение ряда понятий и предъявляемых технических требований, расширение состава сведений об объектах культурного наследия, как дополнительной мере, способствующей улучшению осуществляемых мер по их сохранению.

Ключевые слова: объекты культурного наследия, Единый государственный реестр объектов культурного наследия (памятников истории и культуры) народов Российской Федерации, визуализация, меры по сохранению, цифровые технологии, видеофиксация, лазерное сканирование

PRIVATE LEGAL ASPECTS OF MAINTAINING THE UNIFIED STATE REGISTER OF CULTURAL HERITAGE OBJECTS: THE PROBLEM OF TRADITIONAL AND DIGITAL OBJECT VISUALIZATION TECHNOLOGIES

Abstract. The purpose of the study is to identify the features of maintaining the Register of Cultural Heritage objects (historical and Cultural monuments) of the peoples of the Russian Federation in terms of the use of traditional and the possibility of introducing elements of digital technologies in terms of object visualization. The problem of insufficient elaboration of regulatory legal acts in terms of reflecting a certain composition of information in this register and the requirements imposed on them has been identified. The provision on the closed nature of the list of information entered in the specified register in terms of their visualization is substantiated. It is concluded that it is necessary to adjust the legislation aimed at clarifying a number of concepts and technical requirements, expanding the composition of information about cultural heritage

objects, as an additional measure contributing to the improvement of the measures taken to preserve them.

Keywords: cultural heritage objects, Unified State Register of Cultural Heritage Objects (Historical and Cultural Monuments) of the Peoples of the Russian Federation, visualization, conservation measures, digital technologies, video recording, laser scanning

Введение. Конституцией Российской Федерации [3] и Федеральным законом от 25 июня 2002 г. № 73-ФЗ «Об объектах культурного наследия (памятниках истории и культуры) народов Российской Федерации» (далее – Закон об ОКН) [5] закреплены обязанности и гарантии граждан и государства по сохранению объектов культурного наследия (далее – ОКН).

Такие права и гарантии обеспечиваются, с одной стороны, ведением Единого государственного реестра объектов культурного наследия (памятников истории и культуры) народов Российской Федерации (далее – Реестр) – основным источником сведений об ОКН, с другой – составом этих сведений и возможностью их использования субъектами права, обязанности которых так или иначе затрагиваются данной информацией либо оказывают прямое воздействие на деятельность по сохранению ОКН.

Вместе с тем анализ законодательства Российской Федерации об охране ОКН показывает, что оно обладает рядом положений, требующих дополнения и переработки, в том числе с учетом активного внедрения цифровых технологий. И в особенности в части визуализации ОКН, помещаемой в Реестр.

Исследуемая проблема является многоаспектной, проявляющейся в различных сферах правовых и общественных отношений.

Конституционно-правовой аспект, как особый для цивилистов аспект [6. С. 37], видится в сочетании равнонаправленных обязанностей публичных и частных субъектов в сохранении ОКН.

Гражданско-правовой аспект заключается в том, что, поскольку сведения Реестра в любом случае являются основным источником информации об ОКН, именно они оказывают влияние на весь спектр не только частнособственнических отношений по поводу ОКН, но и, например, договорных аспектов, в рамках которых осуществляются работы по сохранению ОКН.

Публично-правовой аспект обусловлен не только упорядочением деятельности органов власти в рассматриваемой сфере, но и в обеспечении такого баланса публичных и частных интересов, который бы приводил к единой цели – сохранению и охране культурного наследия, основанным на максимально объективных данных о таких объектах.

В этом, между прочим, как отмечал С. А. Шаронов [7. С. 52], и проявляется двойственность понятия «охрана», которое в силу своего содержания характеризуется двойственной правовой природой публичной и частноправовой направленности.

Основная часть. Законом об ОКН закреплено, что Реестр, как государственная информационная система, является основным источником информации

об ОКН. При этом как сам названный нормативный правовой акт, так и принятый в его развитие приказ Министерства культуры РФ от 3 октября 2011 г. № 954 [4], закрепляют закрытый перечень сведений, помещаемых в данный Реестр, к которым относятся фотографические снимки и иные графические изображения (далее – ФСиГИ).

Вместе с тем законодатель не привел понятия данных элементов сведений Реестра, равно как и не обозначил какие же графические изображения возможно использовать в рассматриваемом случае.

Последующая норма Закона об ОКН определяет только лишь общие требования к названным элементам, не раскрывая ни здесь, ни в ином нормативном правовом акте (далее – НПА) их технические требования, руководствуясь только концептуальными положениями о том, что же такие материалы должны содержать.

Иными словами, законодатель, предъявив общие требования к фотофиксации объекта, фактическое исполнение (в отсутствие соответствующих нормативов) отдал на откуп конкретному исполнителю, что не отвечает принципу правовой определенности, необходимость соблюдения которого, в частности, отмечала, например, Е. А. Дербышева [1. С. 29–40; 2. С. 68–79]. Более того, такая правовая конструкция явно может привести к соответствующим судебным разбирательствам, где тяжущиеся стороны явно представят перед судом тот фотографический материал, который отображает правовую позицию одной из сторон с возможным последующим проведением судебной экспертизы, технических ориентиров (требований) для которых не существует.

Следовательно, назрел вопрос не только раскрытия в Законе об ОКН понятий «ФСиГИ ОКН», но и принятия НПА, закрепляющего технические требования к данному элементу Реестра.

Вместе с тем, общий тренд цифровизации всех отраслей хозяйствования подсказывает, что и здесь, не отказываясь от выработанных десятилетиями приемов, по мнению автора, было бы целесообразно дополнить их такими элементами Реестра, как видеофиксация и лазерное сканирование ОКН, что также, естественно, потребует принятия подзаконных НПА, касающихся их технического исполнения.

Именно внедрение таких элементов Реестра, помимо ФСиГИ, позволит детальнейшим образом зафиксировать каждую особенность ОКН. В перспективе именно такой подход будет в полной мере способствовать, во-первых, прямому исполнению нормы Закона об ОКН – сохранению историко-культурной особенности и индивидуальности каждого ОКН, во-вторых, потенциально снимет важнейшую теоретическую и практическую задачу при разработке научно-проектной документации (особенно в условиях некачественных ФСиГИ либо их отсутствия), производстве самих работ по сохранению и их приемке.

В конечном итоге именно такое разрешение исследуемой проблемы, по мнению автора, внесет правовую определенность как в вопросы характеристик предаваемой по договору вещи – ОКН, так и в договорные отношения, связанные с работами по сохранению таких объектов (технические условия, определение необходимых мероприятий по сохранению, исполнение обязательств и пр.).

Помимо прочего, это будет способствовать ясному для всех сторон частно-правовых и публично-правовых взаимоотношений пониманию ценности ОКН в целом и его элементов, возможных способов и приемов сохранения объекта для реализации взаимонаправленной цели – сохранения и передачи будущим поколениям историко-культурного наследия в максимально неизменном виде.

Заключение. В Российской Федерации ведется Реестр, являющийся основным источником сведений об ОКН. При этом перечень сведений носит закрытый характер, а ряд используемых терминов, например, «ФСиГИ», не имеют своего понятийного раскрытия, равно как и требований к их исполнению.

Одновременно с этим в условиях все нарастающего использования цифровых технологий, очевидно, назрела необходимость пересмотра перечня сведений Реестра, направленного на использование технологий видеофиксации и лазерного сканирования ОКН.

Анализ поставленных в публикации вопросов приводит к осознанию необходимости корректировки законодательства Российской Федерации, предложенной автором. Цель корректировок:

1. Внесение изменений в Закон об ОКН посредством введения четкого понятийного аппарата в части ФСиГИ.

2. Дополнение перечня сведений, помещаемых в Реестр видеофиксацией и лазерным сканированием объектов. При этом оба случая потребуют разработки и утверждения отдельными НПА конкретных технических требований к их осуществлению.

Принятие данных корректировок позволит разрешить имеющуюся правовую неопределенность, а также окажет прямое воздействие не только на сами процессы сохранения ОКН, но на весь спектр частноправовых отношений, в которых объектами выступают названные вещи.

Список литературы

1. Дербышева Е. А. Место принципа правовой определенности в системе принципов российского права // Право и политика. 2017. № 2. С. 29-40.

2. Дербышева Е. А. Принцип правовой определенности как требование определенности нормы права // Юридические исследования. 2017. № 2. С. 68-79.

3. Конституция РФ (принята всенародным голосованием 12 декабря 1993 года с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 года) // СПС «КонсультантПлюс».

4. Приказ Министерства культуры РФ от 3 октября 2011 г. № 954 «Об утверждении Положения о Едином государственном реестре объектов культурного наследия (памятников истории и культуры) народов Российской Федерации (ред. от 16 августа 2022 г.) // Бюллетень нормативных актов федеральных органов исполнительной власти. 2012. № 4.

5. Федеральный закон от 25 июня 2002 г. № 73-ФЗ «Об объектах культурного наследия (памятниках истории и культуры) народов Российской Федерации» (ред. от 14 апреля 2023 г.) // Собрание законодательства РФ. 2022. № 26. Ст. 2519.

6. Шаронов С. А. Современное значение и проблемы охранной деятельности в Российской Федерации: цивилистический аспект // Юрист. 2013. № 11. С. 37-40.
7. Шаронов С. А. Концепция гражданско-правового регулирования охранной деятельности в Российской Федерации: монография. М.: Юстицинформ, 2014. 606 с.

К. Г. Сварчевский,
кандидат юридических наук, доцент,
Северо-Западный филиал
Российского государственного университета правосудия
А. Л. Саченко,
кандидат юридических наук, доцент,
Северо-Западный филиал
Российского государственного университета правосудия

ПРОБЛЕМЫ ПРАВОВОЙ КВАЛИФИКАЦИИ ЦИФРОВОГО РУБЛЯ КАК ОБЪЕКТА ГРАЖДАНСКО-ПРАВОВЫХ ОТНОШЕНИЙ: СООТНОШЕНИЕ ЧАСТНО-ПРАВОВОГО И ПУБЛИЧНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. В статье рассматриваются современные проблемы правового режима цифрового рубля как объекта гражданских правоотношений. На основе анализа действующих нормативных правовых актов, демонстрируется неоднозначный подход к пониманию цифрового рубля как объекта правового регулирования с позиции частно-правового и публично-правового законодательства. С целью устранения возможных проблем правовой квалификации режима цифрового рубля предлагается восприятие денежных средств, включая цифровые деньги, в качестве самостоятельного объекта гражданских прав.

Ключевые слова: цифровой рубль, объект гражданских прав, валюта, денежные средства, вещь, имущество, цифровые права

PROBLEMS OF LEGAL QUALIFICATION OF THE DIGITAL ROUBLE AS AN OBJECT OF CIVIL LAW RELATIONS: CORRELATION OF PRIVATE-LAW AND PUBLIC-LAW REGULATION

Abstract. This article considers modern problems of the legal regime of the digital ruble as an object of civil legal relations. Based on the analysis of existing legal acts, the ambiguous approach to the understanding of the digital ruble as an object of legal regulation from the position of private-law and public-law legislation is demonstrated. In order to eliminate possible problems of legal qualification of the digital ruble regime, it is proposed to perceive money, including digital money as an independent object of civil rights.

Keywords: digital ruble, object of civil rights, currency, money, thing, property, digital rights

Современный гражданско-правовой оборот наглядно показал необходимость развития сложившихся платежных систем как с технической, организационной, финансовой, так и с правовой стороны. Развитие цифровой экономики Российской Федерации и ее дальнейшее интегрирование в мировую экономику, безусловно, отражает как общие потребности, так и глобальные процессы, связанные с мировой цифровизацией большинства сфер общественной жизни. В связи с вышеуказанными факторами большое значение имеют вопросы правовой квалификации отношений, складывающихся в цифровой среде, в особенности в системе частно-правовых отношений, в которых средством платежа выступает национальная валюта. Так, одним из факторов данного явления является постепенное вхождение в систему гражданско-правовых отношений такой категории как цифровой рубль. И, хотя анализ данных отношений претендует на значительное количество исследований, как отраслевых, так и межотраслевых, представляется, что выявление особенностей гражданско-правового режима цифрового рубля имеет базовое значение для надлежащей правовой квалификации как со стороны правоохранительных органов, так и различных общественных организаций, представляющих интересы предпринимателей.

С позиции характеристики объектов гражданских прав деньги не выделены в качестве их самостоятельной разновидности, предусмотренной ст. 128 ГК РФ. С одной стороны, это не порождает сколь-либо серьезных проблем с точки зрения восприятия денежных средств исходя из их традиционной дифференциации на наличные и безналичные, с другой – вхождение в качестве объекта гражданских прав цифрового рубля ставит перед законодателем целый комплекс вопросов, требующих разрешения.

Так, согласно, содержанию ст. 128 ГК РФ, наличные деньги по своему правовому режиму приравниваются к вещам, а безналичные деньги законодателем отождествляются с имуществом. Не вдаваясь в детали причин правовой регламентации отнесения двух форм денег к разным, по сути, видам объектов гражданских прав, стоит отдельно в данном контексте упомянуть положение цифрового рубля. Согласно обнародованной на портале ЦБ РФ информации «цифровой рубль – это цифровая форма российской национальной валюты, которую Банк России планирует выпускать в дополнение к существующим формам денег» [1]. При этом ЦБ РФ, выступая в качестве регулятора финансового рынка, рассматривает цифровой рубль в качестве отдельной (цифровой) формы национальной валюты, что также отражено на официальном портале ЦБ РФ [2]. «Цифровой рубль – это третья форма рубля. Сейчас у нас есть наличные (банкноты и монеты в наших кошельках) и безналичные (деньги на счетах в банках, на картах), а в дополнение к ним появится еще и третья форма – цифровая» – именно такая информация объясняет понимание цифрового рубля всем заинтересованным лицам.

На первый взгляд, такое положение вещей вполне объяснимо с позиции того, что согласно ст. 141.1 ГК РФ, цифровыми правами признаются названные в таком качестве в законе обязательственные и иные права, содержание и условия осуществления которых определяются в соответствии с правилами информационной системы, отвечающей установленным законом признакам. В связи с этим следу-

ет сделать промежуточный вывод о том, что легализация такого объекта гражданских прав, как цифровой рубль, порождает возникновение в отношении него цифровых прав. Однако и сама формулировка содержания цифровых прав также оставляет за собой ряд вопросов. Так, в частности, стоит обратить внимание на то, что, указывая обязательственные права в качестве разновидности цифрового права, законодатель расширительно истолковывает содержание цифровых прав, подразумевая то, что под ними могут пониматься и иные права. Вполне логично, что иными правами, возникающими в отношении цифрового рубля, могут быть и вещные права. По крайней мере, никаких ограничений на этот счет в гражданском законодательстве на сегодняшний день не содержится.

И данное заключение представляется вполне логичным в соотношении с содержанием ст. 128 ГК РФ, которая в свою очередь рассматривает наличные деньги в качестве вещей, а безналичные деньги в качестве имущества. В логическую цепочку данного явления органично вплетено и то, что, согласно официальным сведениям ЦБ РФ, содержащимся в Концепции цифрового рубля, цифровой рубль представляет собой обязательство Банка России [3]. В этой связи концепция «цифровой рубль – цифровое право – обязательство» подтверждает свое существование.

Таким образом, четко очерчивается грань между традиционным пониманием наличных и безналичных денежных средств через призму вещно-правовых отношений с точки зрения смысловой нагрузки действующего гражданского законодательства и собственно, цифровых денег, разновидностью которых является цифровой рубль.

Однако данная концепция не может быть реализована ни практически, ни теоретически именно в силу незавершенности процесса регламентации цифрового рубля гражданским законодательством. Об этом, в частности, свидетельствует то, что, согласно проекту № 270852-8 Федерального закона «О внесении изменений в статьи 128 и 140 части первой, часть вторую и статьи 1128 и 1174 части третьей Гражданского кодекса Российской Федерации» безналичные денежные средства дополняются формулировкой «в том числе цифровые рубли». В связи с этим с позиции частноправового регулирования режима цифрового рубля очевидны крайне неоднозначные явления, порождающие проблемы уже на стадии правопонимания правового положения цифрового рубля как разновидности безналичных денежных средств. Таковым, в частности, является на наш взгляд, крайне неудачная правовая конструкция, позволяющая отождествлять цифровой рубль с безналичными денежными средствами.

Данная позиция, несмотря на то, что пока это законопроект, значительно суживает потенциал оборота цифрового рубля. Так, цифровой рубль представляет собой все же средство платежа, размещенного в виде уникального цифрового кода на электронном кошельке [4]. Уже один этот факт выделяет использование цифрового рубля по сравнению с безналичными денежными средствами, для которых наличие такого атрибута, как электронный кошелек, вовсе не обязательно. Более того, подобный подход выходит за рамки гражданско-правового регулирования цифрового рубля в контексте законодательства о национальной валюте.

Исходя из вышеуказанного, согласно положениям ст. 1 Федерального закона от 10.12.2003 № 173-ФЗ (ред. от 31.07.2020) «О валютном регулировании и валютном контроле» [5], валютой РФ признаются: денежные знаки в виде банкнот и монеты Банка России, находящиеся в обращении в качестве законного средства наличного платежа на территории Российской Федерации, а также изымаемые либо изъятые из обращения, но подлежащие обмену указанные денежные знаки, а также средства на банковских счетах и банковских вкладах.

Таким образом, в существенной доработке также нуждается и валютное законодательство, не воспринимающее цифровой рубль как законное средство платежа на территории РФ. Место же среди безналичных и (или) особых цифровых денежных форм остается открытым. В то же время нельзя не отметить и то, что Высший судебный орган РФ – Верховный Суд РФ – придерживается традиционного и даже консервативного воззрения.

Так, например, согласно содержанию Постановления Верховного Суда РФ от 04.09.2015 № 302-АД15-7697 по делу № А74-6846/2014 [6], валютой Российской Федерации признаются денежные знаки в виде банкнот и монеты Банка России, находящиеся в обращении в качестве законного средства наличного платежа на территории Российской Федерации. Хотя при этом нельзя обойти стороной Постановление Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП-16416/2018 по делу № А40-124668/2017, в котором указано, что криптовалюта не может быть расценена применительно к ст. 128 ГК РФ иначе как иное имущество. В принципиально общем подходе к вопросу о квалификации правового режима цифрового рубля в рассматриваемом контексте представляется то, что широкое применение аналогии закона судебными органами с целью правильного и своевременного рассмотрения и разрешения дела вполне допустимо.

Однако вопрос о принадлежности цифрового рубля, который, к слову, не является криптовалютой в общепринятом значении [7], остается открытым, поскольку как было указано выше позиция о том, что цифровой рубль может быть приравнен к иным видам имущества противоречит позиции ЦБ РФ как регулятора рынка финансовых услуг, то есть противоречит публично-правовым началам, определяющим правовой режим цифрового рубля.

Таким образом, при определении гражданско-правового режима цифрового рубля стоит отметить существенные противоречия между публично-правовыми началами и частно-правовыми основами регулирования таких объектов, как денежные средства.

В качестве одного из способов преодоления данных противоречий представляется позитивным рекомендовать возвращение к более привычной классификации объектов гражданских прав, в которых денежные средства поименованы в качестве самостоятельного объекта, без учета их восприятия ни в качестве вещей, ни в качестве имущества. Более детальный подход к дифференциации форм денежных средств как самостоятельной разновидности объектов гражданских прав позволит нивелировать проблемы правоприменения отдельных норм как гражданского, так и валютного законодательства, а также более содержательно воспринимать цифровые отношения в целом с точки зрения теоретического и научного подходов.

Список литературы

1. Концепция цифрового рубля. URL: https://cbr.ru
2. Постановление Верховного Суда РФ от 4 сентября 2015 г. № 302-АД15-7697. URL: https://base.garant.ru
3. Федеральный закон от 10.12.2003 № 173-ФЗ «О валютном регулировании и валютном контроле» // Собрание законодательства РФ. 2003. № 50. Ст. 4859.
4. Цифровой рубль. URL: https://cbr.ru
5. Цифровой рубль: что это такое. URL: https://journal.tinkoff.ru
6. Чем цифровой рубль отличается от криптовалюты. URL: https://cbr.ru

Е. В. Ситкарева,
кандидат юридических наук, доцент,
Всероссийская академия внешней торговли
Министерства экономического развития Российской Федерации
Л. А. Крикун,
кандидат юридических наук, доцент,
Московский финансово-юридический университет

МЕХАНИЗМЫ РАЗРЕШЕНИЯ СПОРОВ НА ПЛАТФОРМАХ ЭЛЕКТРОННОЙ ТОРГОВЛИ: ВОЗМОЖНОСТЬ ИЛИ НЕОБХОДИМОСТЬ?

Аннотация. В статье рассматриваются современные подходы к разрешению споров по сделкам, заключаемым на электронных торговых площадках. Интернет-торговля активно развивается в последнее время, и встает вопрос о необходимости регулирования разрешения споров в данной сфере правоотношений. На основе анализа зарубежного и отечественного опыта сделан вывод, что наиболее эффективным будет внедрение альтернативного механизма урегулирования споров в экосистему, в рамках которой совершаются сделки как между предпринимателями, так и с участием потребителей.

Ключевые слова: альтернативные способы разрешения споров, экосистема, интернет-платформа, электронная торговля

DISPUTE RESOLUTION MECHANISMS ON E-COMMERCE PLATFORMS: OPPORTUNITY OR NECESSITY?

Abstract. The article discusses modern approaches to dispute resolution on transactions concluded on electronic trading platforms. Internet commerce has been actively developing recently, and the question arises of the need to regulate dispute resolution in this area of legal relations. The authors, based on the analysis of foreign and domestic experience, come to the conclusion that the most effective would be the introduction of an alternative dispute settlement mechanism into the ecosystem, within which transactions are made both between entrepreneurs and with the participation of consumers.

Keywords: alternative dispute resolution methods, ecosystem, Internet platform, e-commerce

Современную экономику сложно представить без электронных торговых площадок. Крупнейшая в мире однодневная онлайн-распродажа Global Shopping Festival принесла 120,7 млрд юаней (17,79 млрд долл.) всего за 24 часа на платформах электронной коммерции Alibaba (в основном на сайтах B2C Tmall.com и C2C Taobao Marketplace). Платформы сгенерировали 657 млн заказов на доставку и охватили 235 стран и регионов [11]. Практика показывает, что на онлайн-покупки приходится более 40 % споров, и на трансграничные онлайн-покупки – около 10 % [8]. Очевидно, что с увеличением числа сделок кратно будет возрастать и число споров между участниками. Государственные суды и международный арбитраж объективно не смогут справиться с таким потоком. Да и с учетом цены иска обращение к традиционным способам разрешения споров не видится эффективным.

Юристы, изучающие современные формы альтернативного разрешения споров, такие как «децентрализованное правосудие», отмечают, что современная электронная коммерция выдвинула на передний план новую категорию споров, а именно мелкие транснациональные споры, при этом традиционные механизмы, включая государственные суды, плохо подходят для разрешения таких споров [7].

Всплеск электронной торговли привел к возникновению десятков миллионов споров на площадках электронной торговли – интернет-платформах. Безусловно, ни в одной стране не было ни миллиона арбитров, ни миллиона медиаторов для разрешения указанных споров. Так, на платформах онлайн-торговли первоначально в США и Европе (eBay, Amazon, Modria), затем в Китае (Alibaba), вне регуляторного вмешательства государства, появляются платформы онлайн-разрешения споров [3].

Еще в далеком 1999 г. eBay обратилась к Центру исследований информационных систем Массачусетского университета с просьбой осуществить экспериментальный проект по медиации. Пилотный проект обработал 200 споров в течение двухнедельного периода. Этот положительный опыт привел к тому, что на eBay включили разрешение споров в качестве опции для покупателей и продавцов, в случае если сделка оказалась неудачной. За 10 лет количество споров, рассмотренных на площадке eBay, достигло ошеломляющего числа в 60 млн.

Созданы и действуют различные системы со своими правилами и особенностями. К ключевым игрокам относят: Kleros, Aragon и Jur. Так, Клерос позиционирует себя как децентрализованный арбитражный сервис для споров новой экономики [15]. Суд Арагон (Aragon Court) на основе протокола децентрализованного разрешения споров – подключаемая арбитражная платформа, легко доступная для любого децентрализованного приложения – к своим преимуществам относит «возможность для людей со всего мира получить доступ к разрешению спора с большим удобством и меньшими затратами, чем в традиционных судах» [14].

К основным характеристикам указанных форм альтернативного разрешения споров, пожалуй, следует отнести то, что данные механизмы реализованы в рамках отдельных экосистем и, по сути, являются замкнутыми для пользователей, что обеспечивает исполнимость решений. В зависимости от сложности спора на платформах предложены различные правовые инструменты.

Основными преимуществами выступают высокая скорость разрешения спора и низкая стоимость.

В качестве примера можно рассмотреть процедуру Центра разрешения споров пользователей Taobao (Taobao Marketplace принадлежит гиганту электронной коммерции Alibaba Group). Китайская корпорация Alibaba, имеет крупнейший в мире рынок B2B (business-to-business) – Alibaba, крупнейший в мире рынок C2C (consumer-to-consumer) – Taobao, крупнейший внутренний рынок B2C (business to consumer) – Tmall и платежный инструмент – «Alipay» [12]. Система Taobao компании Alibaba Group в настоящее время является крупнейшей в мире платформой электронной коммерции для потребителей [2]. С платформой сотрудничают более 10 млн активных продавцов и 423 млн активных покупателей. Участники спора излагают свои позиции на онлайн-форуме, жюри из 31 присяжного (в качестве присяжного могут выступать пользователи, зарегистрированные на платформе не менее года) изучает их до вынесения решения. Решение выносится простым большинством голосов. Для присяжных не установлен гонорар, они осуществляют эту деятельность бесплатно [10]. Crowd-sourced cyber-jurie, как утверждают исследователи, начал развиваться еще в 90-е годы XX века [13].

В целом различные системы вполне вписываются в рамки механизмов альтернативного разрешения споров, и в большинстве стран мира на современном этапе государственные регуляторы не видят необходимости дополнительного регулирования, включая определенные императивы. В то же время следует обратить внимание на опыт Китая, особенно с учетом локализации электронных торговых площадок.

Законодательство КНР достаточно жестко регулирует порядок онлайн-урегулирования споров частными платформами электронной торговли. Статья 63 Закона КНР об электронной торговле 2019 г. (E-Commerce Law, далее – ECL) позволила операторам электронной торговли создавать собственные онлайн-системы разрешения споров [9]. Согласно ECL, платформы электронной торговли должны своевременно принимать и рассматривать любые жалобы и сообщения, для чего обязаны обеспечить удобные и эффективные механизмы подачи жалоб и сообщений. Конечно, указанный закон предусматривает возможность обращения к любым способам разрешения споров, включая переговоры, медиацию, арбитраж или судебное разбирательство, в то же время искомая эффективность может быть достигнута лишь путем внедрения механизма разрешения споров в экосистему электронной торговли.

В России, как ни парадоксально, с активным развитием платформ интернет-торговли, популярностью и развитием экосистем, названия которых у всех на слуху, регулирование разрешения споров из таких отношений скорее стагнирует, чем развивается.

Как известно, платформы электронной торговли в нашей стране не содержат внутренних систем урегулирования споров. Можно встретить лишь отдельные ресурсы для предъявления претензий/вопросов, на которые можно получить скупой шаблонный ответ. Нормативные акты не требуют эффективной системы реагирования на возникающие спорные ситуации.

Более того, проект ФЗ № 1138398-7 «О внесении изменений в Закон РФ "О защите прав потребителей" и ФЗ "Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)"» 2021 г. таких требований также не содержит. В пояснительной записке к законопроекту указывалось, что Роспотребнадзор в докладе 2016 г. отмечал «ежегодный прирост жалоб потребителей в отношении хозяйствующих субъектов, чья деятельность по продаже товаров осуществляется посредством сети Интернет» [4]. Примечательно, что в дальнейших отчетах Роспотребнадзора фиксируется уже не увеличение количества жалоб, а лишь увеличение рынка интернет-торговли [1]. Согласно документу, досудебные споры могут быть урегулированы через портал «Госуслуги». Есть вероятность, что планируется создать единый онлайн-центр для разрешения споров в сфере интернет-торговли [5]. Законопроект № 1138398-7 был принят в первом чтении Госдумой в 2021 г. и с тех пор его рассмотрение постоянно откладывается [6]. Нельзя не отметить разнонаправленность действий со стороны государства в данном случае. С одной стороны, угадывается желание или потребность контролировать процессы урегулирования споров между участниками интернет-торговли, определенную степень недоверия альтернативным способам урегулирования споров, что уже показала и реформа третейского разбирательства, с другой – недостаточность внимания или возможностей для реализации такого намерения.

Развитие площадок интернет-торговли стало объективной реальностью. Имеются неоспоримые преимущества как для предпринимателей, так и для потребителей. Система государственного правосудия не сможет обеспечить в должной мере эффективность разбирательства возникающих споров, как и традиционные альтернативные способы урегулирования споров. Зарубежный опыт в этой сфере демонстрирует, что наиболее эффективной для участников может стать внутренняя система разрешения споров на самих электронных площадках, интегрированная в экосистемы. В то же время следует понимать, что любые дополнительные возможности для пользователей влекут расходы для держателей такого программного обеспечения, и они не всегда могут быть заинтересованы в развитии отдельных направлений. Поэтому государству в целях в том числе экономии бюджетных средств на разрешение споров следует стимулировать, в частности, нормативными требованиями создание отдельных механизмов урегулирования споров между участниками – пользователями электронных площадок интернет-торговли, как предпринимателями, так и потребителями.

Список литературы

1. Государственный доклад «Защита прав потребителей в Российской Федерации в 2021 году». URL: https://www.rospotrebnadzor.ru

2. Ермакова Е. П. Онлайн-разрешение споров на китайской платформе электронной торговли «Taobao» // Территория новых возможностей. Вестник Владивостокского государственного университета экономики и сервиса. 2022. Т. 14, № 3. С. 118-128.

3. Ермакова Е. П. Особенности онлайн-урегулирования потребительских споров платформами электронной торговли в Китайской Народной Республике // Journal of Digital Technologies and Law. 2023. Т. 1, № 3. С. 691-711. EDN OZHVUE

4. Законопроект № 1138398-7 «О внесении изменений в Закон Российской Федерации „О защите прав потребителей“ и Федеральный закон „Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)“ в части создания правовой основы для развития системы альтернативных онлайн-механизмов урегулирования споров». URL: https://sozd.duma.gov.ru/bill/1138398-7

5. Мельник В. Д. О создании онлайн-сервиса урегулирования потребительских споров в Российской Федерации // Арбитражный и гражданский процесс. 2022. № 7. С. 58-59. EDN: CQVOQP

6. Статус законопроекта № 1138398-7 О внесении изменений в Закон Российской Федерации «О защите прав потребителей» и Федеральный закон «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)» в части создания правовой основы для развития системы альтернативных онлайн-механизмов урегулирования споров. URL: https://sozd.duma.gov.ru/bill/1138398-7

7. Aouidef Y., Ast F., Deffains B. Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects // Front. Blockchain. 2021. Vol. 4. Art. 564551.

8. CECRC 2015 Annual Report on Consumer's Experience and Complaints Monitoring of China E-commerce. URL: www.100ec.cn

9. E-Commerce Law of the People's Republic of China (Adopted at the Fifth Session of the Standing Committee of the 13th National People's Congress. URL: https://ipkey.eu

10. How Taobao Is Crowdsourcing Justice in Online Shopping. URL: https://www.alizila.com

11. Juanjuan Z. Chapter 10. On China Cross-Border Online Dispute Settlement Mechanism-Following UNCITRAL Tnodr and Alibaba Experience. URL: https://www.wgtn.ac.nz

12. Liu L. and Weingast B. Taobao, Federalism, and the Emergence of Law, Chinese Style. URL: https://scholarship.law.umn.edu/mlr/111

13. Sela A. The Effect of Online Technologies on Dispute Resolution System Design: Antecedents, Current Trends and Future Directions // Lewis & Clark Law Review. 2017. № 21. Pp. 633-680.

14. Сайт платформы Арагон. URL: https://aragon.org/aragon-court

15. Сайт платформы Клерос. URL: https://kleros.io

А. В. Тумаков,
кандидат юридических наук, доцент,
Московский университет Министерства внутренних дел
Российской Федерации имени В. Я. Кикотя

ПЕРСПЕКТИВЫ ФОРМИРОВАНИЯ ЦИФРОВОГО ПРАВА В ОТЕЧЕСТВЕННОЙ ПРАВОВОЙ СИСТЕМЕ

Аннотация. Предметом исследования выступают цифровые правоотношения. Цель исследования – проанализировать складывающиеся правоотношения в цифровой среде и определить их характерные особенности. Исследование проведено с применением общенаучных методов, таких как анализ, синтез и абстрагирование. В статье делается вывод, что из всех характерных признаков цифрового правоотношения ключевыми (конституирующими) являются наличие особой сферы (информационной, где возникают, изменяются и прекращаются правоотношения) и использование цифровых технологии как средств, обеспечивающих осуществление прав и исполнение обязанностей.

Ключевые слова: цифровое право, цифровое правоотношение, цифровые технологии, цифровизация, информационные системы

PROSPECTS FOR THE FORMATION OF DIGITAL LAW IN THE DOMESTIC LEGAL SYSTEM

Abstract. The subject of the study is digital legal relations. The purpose of the study is to analyze the emerging legal relations in the digital environment and determine their characteristic features. The study was carried out using general scientific methods such as analysis, synthesis and abstraction. The article concludes that of all the characteristic features of a digital legal relationship, the key (constitutive) ones are the presence of a special sphere (informational, where legal relationships arise, change and terminate) and the use of digital technologies as a means of ensuring the exercise of rights and the fulfillment of obligations.

Keywords: digital law, digital legal relations, digital technologies, digitalization, information systems

Любое правоотношение, как форма реализации права, характеризуется своим субъектом, объектом и содержанием (правами и обязанностями сторон). С этих позиций цифровое правоотношение не отличается от иных правоотношений, имеющих сходный объект. Например, договор купли-продажи товара, заключенный непосредственно в магазине или на интернет-площадке с использованием цифровых технологий, имеют один и то же объект в виде получения в собственность того или иного материального блага (товара); определенный состав субъектов (продавца и покупателя); сходное содержание. Таким образом, структура цифрового правоотношения не отличается от «традиционного» правоотношения». Однако есть и различия:

– взаимодействие осуществляется в информационной среде;

– средством, способствующим осуществлению прав и исполнению обязанностей, являются цифровые технологии;

– покупатель и продавец находятся территориально в разных местах и могут не иметь представления о месте нахождения друг друга, что с позиции права затрудняет определение места передачи товара, предъявление претензий, направление уведомлений и пр.;

– субъекты хотя и проходят идентификацию, но достоверно установить их личности, как правило, невозможно;

– влияние на возникающие правоотношения могут оказывать субъекты, являющиеся обладателями прав на электронные площадки, где стороны вступают в правоотношения. В целом круг участников цифрового правоотношения шире «традиционного». Сюда можно включать и субъектов, осуществляющих доступ к сетевым протоколам и веб-сервисам, и информационных посредников, и др.

Все указанные факторы формируют особенности цифрового правоотношения.

В контексте понятий «цифровой» – «аналоговый» идет противопоставление всему, что было в доцифровую эпоху. Ошибочно будет анализировать период в несколько столетий формирования и становления правовых систем в сравнении с последним десятилетием.

Цифровизация, как и информатизация, – это процессы, которые вовлечены во все сферы общественной жизни в качестве технических решений, автоматизируют процессы, и они характерны лишь для небольшого промежутка времени по меркам человеческой истории и права в целом. Безусловно, право будет адаптироваться под меняющиеся правоотношения, но провести четкую грань между цифровыми и другими правоотношениями нельзя. В каждых правоотношениях рано или поздно появится цифровой компонент. Начиная от электронных покупок в маркетплейсах, заканчивая получением госуслуг через приложение, не выходя из дома. Однако это скорее эволюция, а не революция, как многим хотелось бы представить.

Если немного углубиться в цифровые правоотношения, то можно заметить, что в них обязательно будет прослеживаться некий цифровой элемент: либо средство реализации прав и исполнения обязанностей, либо специфическая среда. Например, реализовывать свои цифровые права в широком смысле можно с помощью привычного смартфона – это в первую очередь доступ к сети Интернет. Однако в узком смысле цифровые права – это особые объекты гражданских прав, предусмотренные ст. 141.1 ГК РФ, к которым относятся цифровые финансовые активы и утилитарные цифровые права. Законом предусмотрены специальные субъекты, например, оператор инвестиционной платформы или лицо, привлекающее инвестиции. Поскольку они вступают в правоотношения по поводу цифровых прав, их можно назвать цифровыми.

Из всех перечисленных выше признаков цифрового правоотношения ключевыми (конституирующими) являются наличие особой сферы (информационной, где возникают, изменяются и прекращаются правоотношения) и использование цифровых технологий как средств, обеспечивающих осуществление прав и исполнение обязанностей. Именно эти факторы позволяет утверждать, что речь идет о цифровом правоотношении.

Указанные признаки, в свою очередь, влияют на содержание правоотношения. Например, если в «традиционном» правоотношении при отсутствии указания места передачи товара можно воспользоваться общим указанием закона, то в цифровом правоотношении руководство общими положениями может привести к невозможности исполнения обязательства в том случае, например, если продавец находится в Китае, а покупатель в России. Следовательно, в цифровом правоотношении появляется совокупность условий (существенных условий), которые необходимо согласовать и которые непосредственно влияют на исполнение обязательства.

Что касается различий по объекту, то наличие цифрового аспекта никак не влияет ни на объект правоотношения, ни на нахождение цифрового правоотношения в той или иной классификационной группе. В этом аспекте цифровые правоотношения систематизируются по тем же основаниям, что и «традиционные» правоотношения (имущественные и неимущественные, абсолютные и относительные и пр.).

Даже в тех ситуациях, когда объектом правоотношения выступает цифровой товар (например, цифровое право), ни структура правоотношения, ни видовая принадлежность правоотношения не меняются. В данном случае, исходя из того, что цифровое право – имущественное право, это будут имущественные правоотношения.

Как уже отмечалось ранее, в данных правоотношениях должен прослеживаться «цифровой» элемент. В широком смысле это либо средства реализации гражданской правосубъектности в цифровой среде, сама цифровая среда (онлайн-платформы, сервисы, маркетплейсы и т. д.), либо специфические объекты, как, например, криптовалюты, NFT, искусственный интеллект и пр.

Гражданское право, включая теорию правоотношений, возникло задолго до появления цифровых технологий. Однако современное право не может не учитывать ту специфику, которую порождает их использование.

Право не оторвано от жизни, в его основе лежат социально-экономические условия, которые являются базисом для формирования норм права. Диалектика права заключается в необходимости учета влияния цифровых технологий на возникновение, изменение и прекращение правоотношений. В рамках существующих институтов права необходимо учитывать особенности цифровых правоотношений. Для устранения пробелов должны появляться и новые институты, посвященные регулированию исключительно цифровых объектов.

Здесь мы имеем двухсторонний процесс. Исходя из того, что цифровые правоотношения имеют традиционную структуру в ряде случаев, при минимальном изменении норм права возможно встроить их правовое регулирование в существующие институты права. С другой стороны, как сказано выше, появление новых отношений непосредственно отражается на правовом регулировании и требует создания новых правовых норм. Таким образом, происходит интерференция права и цифровизации.

Таким образом, определенно право меняется в условиях цифровизации. В качестве примера можно указать создание логически непротиворечивых и одно-

значно понятных машиночитаемых текстов законов. Также поскольку право в первую очередь регулирует поведение людей, оно должно дать определенные рамки субъектам, в которых они будут находиться в цифровых реалиях, а также описать последствия выхода за них. Например, заражение вредоносной программой-вирусом чужого устройства – уже давно уголовно наказуемое деяние, хотя ранее никто и думать не мог о таком способе совершения преступления. Особую роль в процессе цифровизации играет охрана персональных данных, следовательно, законодательство в данной сфере также будет развиваться. Можно сказать, что цифровизация – это тренд, в соответствии с которым будет развиваться и право, однако на смену ему обязательно придет другой. И мы уже будем говорить, например, о тенденциях трансгуманизации и объединения сознания человека с машиной, однако не будем забегать далеко вперед.

С учетом отсутствия в цифровом правоотношении признака национальной принадлежности возможности нахождения субъектов в различных государствах затруднительно определить юрисдикцию (право той страны, которое подлежит применению). Невозможно, как правило, использовать и нормы международного частного права о месте вступления в правоотношения, совершения договора и пр. Значительно осложняются правоотношения и когда в них принимает участие посредник (интернет-площадка), имеющая собственную юрисдикцию, отличную от юрисдикций сторон правоотношения. Таким образом, определить применимое право зачастую невозможно. Из этого, на наш взгляд, следует, что в целях регулирования цифровых правоотношений право государств будет сближаться, будут вводиться общие институты права, учитывающие специфику взаимодействия в виртуальном мире.

Безусловно, могут возникнуть общемировые стандарты, например, по осуществлению расчетных операций стейблкоинами между государствами. Однако этому должен предшествовать международный договор. Например, каждый день совершаются тысячи международных авиарейсов, однако правила их совершения приведены к определенным стандартам, которые отражены в том числе в Чикагской конвенции о международной гражданской авиации.

На начальном этапе разные государства будут выстраивать свои системы законодательства, и, возможно, чей-то правовой режим окажется более прогрессивным и удобным, поэтому данный опыт подхватят остальные. Однако говорить об общемировых трендах пока не приходится. К примеру, очень остро стоит вопрос о противодействии отмыванию доходов, полученных преступным путем, с использованием криптовалют. Однако соответствующие стандарты противодействия и надзорные инстанции созданы не в каждом государстве, не говоря уже о создании международного договора или специальной организации.

А. Е. Туманова,
аспирант,
Финансовый университет
при Правительстве Российской Федерации

ПРОБЛЕМЫ СОЗДАНИЯ ЦИФРОВЫХ ЭКОСИСТЕМ КРЕДИТНЫХ ОРГАНИЗАЦИЙ: ПРАВОВЫЕ АСПЕКТЫ

Аннотация. В последние годы одной из тенденций является существенное усложнение принципов построения бизнес-структур. Наиболее актуальным трендом современности выступает повышенный интерес к формированию экосистем, посредством которых организуется финансово-хозяйственная деятельность компаний и реализуются их бизнес-стратегии развития. В статье предлагается определение цифровой экосистемы кредитной организации, проводится анализ условий создания кредитными организациями цифровых экосистем, а также рассматриваются основные причины высокого интереса со стороны кредитных организаций к реализации экосистемного подхода.

Ключевые слова: цифровизация, цифровые экосистемы, цифровые технологии, кредитные организации, правовые аспекты

PROBLEMS OF CREATING DIGITAL ECOSYSTEMS OF CREDIT INSTITUTIONS: LEGAL ASPECTS

Abstract. In recent years, one of the trends is a significant complication of the principles of building business structures. The most relevant trend of our time is the increased interest in the formation of ecosystems through which the financial and economic activities of companies are organized and their business development strategies are implemented. The article proposes a definition of the digital ecosystem of a credit institution, analyzes the conditions for the creation of digital ecosystems by credit institutions, and also examines the main reasons for the high interest from credit institutions in the implementation of the ecosystem approach.

Keywords: digitalization, digital ecosystems, digital technologies, credit organizations, legal aspects

Стремительное проникновение во все сферы жизни цифровых технологий способствовало эволюционированию форм осуществления финансово-хозяйственной деятельности. При этом происходит значительный рост объемов информации, а также меняются методы ее обработки [6].

Большое разнообразие потоков информации и их обработка требуют повышения эффективности формирования и развития экосистем цифрового типа, которые нашли широкое распространение в банковском секторе экономики [10].

С правовой точки зрения, экосистема – это динамично развивающаяся сеть, которая формируется посредством организаций, индивидов и требует обеспечения бесперебойной и надежной связи между ее отдельными элементами посредством цифровой платформы для достижения поставленных целей и задач, получения экономической выгоды, а также внедрения инновационных решений [5].

В соответствии с Решением Высшего Евразийского экономического совета от 11.10.2017 № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года» цифровая экосистема – это устойчивая система открытого типа, которая включает в себя субъектов экосистемы цифрового типа (виртуальных, юридических, физических), а также установившиеся между ними отношения и связи, реализующиеся посредством сервисов цифровой платформы [1].

В Концепции общего регулирования деятельности групп компаний, развивающих цифровые сервисы на базе одной «экосистемы», цифровая экосистема рассматривается как клиентоориентированная модель организации бизнеса, объединяющая несколько групп продуктов и услуг для удовлетворения потребностей клиентов [2].

Иное определение данного понятия содержится в докладе Банка России «Экосистемы: подходы к регулированию», где под экосистемой (цифровой экосистемой) понимается совокупность платформенных сервисов компании и партнеров, позволяющих клиентам получать широкий спектр товаров и услуг на базе единой цифровой (технологической) платформы [3].

В научной литературе отмечается, что формирование кредитными организациями экосистем требует выполнения следующих условий:

1. Наличие у кредитной организации большой клиентской базы и досконального изучение кредитной организацией предпочтений и потребностей клиентов. Это дает возможность кредитной организации реализовать продуктовую линейку услуг индивидуального характера, максимально удовлетворяющую все сегменты рынка. Кроме этого, также повысить уровень конкурентоспособности кредитной организации посредством расширения предложения продуктов и получения от партнеров различных услуг и сервисов [7].

2. Реализация цифровой экосистемы подразумевает оцифровку всех бизнес-процессов кредитной организации посредством использования ИТ-технологий. Искусственный интеллект, Big Data и другие цифровые технологии в полной мере заменяют прежние традиционные механизмы в реализации продуктов и услуг в целях создания эффективного маркетплейса пользовательских сервисов [4].

3. Наличие цифрового интерфейса и пользовательских якорных сервисов.

4. Взаимодействие кредитной организации с компаниями-партнерами, обеспечивающих создание предложения в части нефинансовых сервисов и услуг для клиентской базы [9].

Рассматривая основные причины высокого интереса со стороны кредитных организаций к реализации экосистемного подхода, можно отметить следующие:

1. В первую очередь необходимо констатировать, что кредитные организации на сегодняшний день достигли предельных показателей в развитии финансовых сервисов, что привело к еще большему обострению конкуренции на рынке финансовых услуг. Практически все ниши оказались охваченными, в связи с этим возникла необходимость поиска дополнительных конкурентных преимуществ для дальнейшего развития путем внедрения инновационных решений и стремления к повышению разнообразия и качества сервиса [8].

2. Кредитным организациям в условиях нестабильности внешней среды требуются новые источники доходов, этого можно добиться посредством реализации нефинансовых сервисов. При этом важным условием является обеспечение необходимого уровня лояльности клиентов кредитной организации [11].

3. Формирование кредитными организациями экосистем, с одной стороны, сопряжено с созданием мощных барьеров для входа на рынок других участников, но с другой – это стимулирует кредитные организации к развитию и диверсификации как финансовых, так и нефинансовых продуктов и услуг.

Подводя итог, цифровую экосистему кредитной организации можно охарактеризовать как форму организации бизнеса интегрированного типа кредитной организацией, в основе которого лежит применение одной или нескольких платформ цифрового характера с большим количеством сервисов, которые объединяют поставщиков услуг и клиентов для удовлетворения потребностей как финансового, так и нефинансового характера.

Полагаем, что в будущем развитии банковского бизнеса будет превалировать именно экосистемный подход. Активное использование кредитными организациями цифровых технологий, в особенности технологии больших данных, позволяет обеспечить формирование разнообразных клиентских сервисов с концентрацией на клиенте и его потребностях [12].

Список литературы

1. Решение Высшего Евразийского экономического совета от 11 октября 2017 г. № 12 «Об Основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года». URL: https://docs.eaeunion.org

2. Концепция общего регулирования деятельности групп компаний, развивающих цифровые сервисы на базе одной «экосистемы». URL: https://www.economy.gov.ru

3. Доклад для общественных консультаций ЦБ. Экосистемы: подходы к регулированию. URL: https://www.cbr.ru

4. Дяченко О. Финансовая экосистема: все в одном // Национальный банковский журнал (NBJ). 2018. № 5. С. 83-95.

5. Зубок С. Финтех-акселерация как способ внедрения инновационных решений и сервисов в банковскую деятельность // Банковский вестник. 2020. № 9(686). С. 28-37.

6. Панова Г. С., Трушина К. В. Бизнес-стратегии крупнейших банков в области финтех // Банковские услуги. 2019. № 3. С. 4.

7. Розенберг Г. С. Бизнес-экосистемы: что стоит за словами и куда это ведет? // Междисциплинарный научный и прикладной журнал «Биосфера». 2020. Т. 12, № 4. С. 162-175.

8. Ткачев В. Н., Перцева С. Ю. Трансформация регулирования финансовых рынков в цифровой экономике // Развитие современной экономической науки: проблемы, тенденции, перспективы: материалы Международной научной конференции / под ред. К. К. Кумехова и др. М.: Одинцовский филиал МГИМО МИД России, 2019. С. 218-222.

9. Ушанов А. Е. Банковские экосистемы: плюсы, минусы, перспективы развития // Креативная экономика. 2022. Т. 16, № 4. С. 1486-1496.

10. Филимонов И. В. Экосистема цифровой экономики: проблемы предметной идентификации // Инновации и инвестиции. 2020. № 6. С. 52-60.

11. Шакер И. Е. Архитектура элементов цифровизации банка: направления развития // Финансы, деньги, инвестиции. 2020. № 1. С. 38-50.

12. Щербакова Н. В. Цифровые технологии в банковском секторе РФ: особенности и сопутствующие угрозы // Вестник Кемеровского государственного университета. Серия: Политические, социологические и экономические науки. 2021. Т. 6, № 1. С. 137-152.

Н. А. Усольцева,
кандидат юридических наук, доцент,
Сургутский государственный университет
Ю. М. Усольцев,
доцент,
Сургутский государственный университет

МЕТАВСЕЛЕННАЯ КАК МЕСТО ИСПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВА: ПРАВОВЫЕ АСПЕКТЫ

Аннотация. Развитие современных технологий меняет наш мир не только в реальности, изменения происходят и в самом виртуальном пространстве. Новый уровень развития интернет-технологий, расширение реального мира внутрь виртуального пространства, более тесная связь реального и виртуального мира и, как следствие, появление метавселенных ставят перед юристами новые вопросы и формируют запрос к государствам о необходимости уточнения правовых норм. Не стало исключением и гражданское право, где значительная часть обязательств стала гибридом, существующим одновременно в обоих мирах. Отдельные вопросы исполнения обязательства, а именно определение места исполнения обязательства, связанного с метавселенной, и стали предметом исследования настоящей статьи. Методологическую основу данного исследования составляет совокупность методов научного познания, а именно общенаучные и частнонаучные методы исследования, в частности формально-юридический, сравнительно-правовой, технико-юридический. В результате исследования делается вывод о возможности определения местом исполнения обязательства метавселенной на договорном уровне уже в современном состоянии законодательства и определяются перспективы такого места исполнения обязательства в силу закона.

Ключевые слова: метавселенная, место исполнения обязательства, гражданско-правовое обязательство, виртуальное пространство

THE METAVERSE AS A PLACE OF PERFORMANCE OF OBLIGATIONS: LEGAL ASPECTS

Abstract. The development of modern technologies is changing our world not only in reality, but changes are also taking place in the virtual space itself. A new level of development of Internet technologies, the expansion of the real world into the virtual space, a closer connection between the real and virtual worlds, and as a result the emergence of metaverses, raise new questions for lawyers and form a request to states about the need to clarify legal norms. Civil law was no exception, where a significant part of the obligations became a hybrid that exists simultaneously in both worlds. Separate issues of fulfillment of an obligation, namely the determination of the place of fulfillment of an obligation associated with the metaverse, became the subject of this article. The methodological basis of this study is a set of methods of scientific knowledge, namely, general scientific and private scientific methods of research, in particular formal legal, comparative legal, technical legal. As a result of the study, the authors conclude that it is possible to determine the place of fulfillment of the obligation of the metaverse at the contractual level already in the current state of legislation, and determine the prospects for such a place of fulfillment of the obligation by virtue of the law.

Keywords: metaverse, place of fulfillment of an obligation, civil law obligation, virtual space

Введение. Современное развитие цифровых технологий вносит существенные коррективы не только в фактическую действительность взаимодействующих субъектов, но и в систему правового регулирования их отношений. Уже привычным является исследовательский интерес к правовому определению электронных субъектов, к цифровым следам и смарт-контрактам, но развитие технологий не стоит на месте, и происходит расширение их развития уже в сугубо отраслевом векторе.

Гражданское право не стало исключением из указанного процесса расширения и все больше его институтов становятся связанными с цифровыми технологиями в своем существе. Базовая теория гражданского права об обязательствах всегда являлась классикой цивилистики, изменения которой наименее всего подвержены внешнему влиянию и зачастую ориентированы исключительно на концептуальные изменения права. Но развитие цифровых технологий исподволь создало ситуацию, когда концептуально изменения не требуются, но вопросы, требующие уточнения в понимании привязки к ним, формируются.

Основная часть. Один из базовых постулатов гражданского права определяет, что обязательство должно исполняться в надлежащем месте. В классической цивилистике место исполнения обязательства – это некое географическое место, привязанное к сторонам обязательства либо в силу закона или в силу договора, либо в силу обычая или существа обязательства.

Если невозможно определить место исполнения обязательства, то Гражданский кодекс Российской Федерации (далее – ГК РФ) в ст. 316 предлагает установленные правила определения надлежащего места. Данные правила ориен-

тированы на место нахождения недвижимости, место нахождения или хранения, изготовления имущества в привязке к другим обязательствам, месту нахождения субъекта отношений (или места жительства). Если же субъекты отношений или сами отношения сформированы и реализуются в киберпространстве, то как можно определить место исполнения обязательства и какими правовыми признаками оно может быть определено?

Исходно определим, что киберпространство как метафорическая абстракция или виртуальная реальность однозначно уже воспринимается как место в системе правовых координат, но в привязке к точной категории «место исполнение обязательства» этого недостаточно. Необходимо более точное цикличное законченное понятие, которое можно было бы использовать в соединении места исполнения обязательства и киберпространства. На пространстве цифровой терминологии не так давно (Лавина (Snow Crash), 1992 г.) появилось новое определение места, и это метавселенная (metaverse, или метамир).

Насколько же можно использовать метавселенную как место исполнения обязательства с возможностью ее привязки к нормативным конструкциям, существующим в современном гражданском законодательстве России?

Для начала определим метавселенную с позиции юриспруденции и дадим ей правовую характеристику. Метавселенная – это своеобразный мир между мирами (слово «метавселенная» образовано от приставки греч. μετά- (между, после, через) и слова «вселенная» (что иначе означает мир)) [1] или трансцендентный мир. Более приближенно к юриспруденции метавселенную можно определить как пространство, сочетающее реальный и виртуальный мир в рамках одной платформы, где создается самостоятельная реальность со своими правилами, условиями и субъектами. Субъекты, взаимодействующие через метавселенную, существуют в виде аватаров, цифровых личностей и цифровых двойников. Метавселенная является симбиозом физической, дополненной и виртуальной реальности [3. С. 2–7].

Существующие подходы оценивают метавселенную как экосистему виртуальной реальности, сочетающую разнообразные технологии [9. С. 1–7]. Существующая на сегодня концепция Web3 предположительно будет определять развитие Интернета по следующим направлениям: децентрализация; искусственный интеллект и машинное обучение; открытость; свобода; вездесущность; семантическая паутина [7]. Получается, что метавселенная как перспективное направление развития Интернета и виртуальности должна соответствовать данным характеристикам. В качестве уже закономерных называются такие характеристики метавселенной, как иммерсивность, многомерность, устойчивость, интероперабельность, масштабируемость, неоднородность [3. С. 2–7].

На этой логике построено две концепции метавселенной как виртуальной платформы. Первая метавселенная – децентрализованная, предоставляющая права собственности и новые возможности, интероперабельная, открытая и принадлежащая участникам. Вторая, соответственно, прямая ей противоположность – закрытая, централизованная, принадлежащая конкретным лицам [5].

Если метавселенная может быть корпоративной по сути своей, то совсем не обязательно, чтобы владелец использовал ее исключительно для продуктовых

решений. Возможно, часть финансово-хозяйственной деятельности владельца метавселенной перенесена из реального мира именно туда, с организацией там рабочего пространства (даже созданием соответствующих рабочих мест в метавселенной и приемом на работу реальных физически существующих людей через их аккаунты, аватары, учетные записи и т. д.).

Все это делает метавселенную чрезвычайно похожей на платформу блокчейн со всеми ее характеристиками и разновидностями, и приводит к логическому выводу, что метавселенная – децентрализованная платформа, это виртуальный мир, основанный на технологии блокчейн. Метавселенная может создаваться как виртуальное продолжение реального мира, а может создавать абсолютно иллюзорный нереальный мир, например, для компьютерных игр. И в этой связи формируется два кластера сделок – реальные сделки (создающие обязательства в реальном мире), совершенные на платформе метавселенной; и сделки метавселенной (создающие основное обязательство в метавселенной), но имеющие продолжение в реальности.

Какова будет концепция реальной сделки в такой ситуации? Сразу определимся, что реальность в этой ситуации обозначает, что суть обязательства принадлежит исключительно реальному (физическому) миру. В такой ситуации возможно, что и подписание трудового договора, и оформление иных сделок будут проходить именно на платформе метавселенной. Географически метавселенную в такой ситуации можно определить в привязке к компании-правообладателю или собственнику соответствующей метавселенной и его юрисдикции. Договор в такой ситуации должен четко идентифицировать привязку к метавселенной и смысл этой связи – именно место заключения договора. Само обязательство по данной сделке остается в реальном мире, и такая концепция максимально близка идее и логике смарт-контракта.

Сделки метавселенной имеют практически обратную логику и могут обретать договорную форму и на платформе, и в реальности, но само обязательство в принципе существует и исполняется внутри метавселенной, например, когда приобретается виртуальная недвижимость внутри метавселенной [8], приобретаются права пользования, действующие в рамках метавселенной, покупается целый готовый мир (разработанная метавселенная) [7]. Естественно, что в рамках данной концепции место исполнения обязательства и основная часть самого обязательства определяются рамками метавселенной. Несомненно, что такие сделки имеют последствия в реальном мире, так как лицо или компания, получившие какие-то права или имущество в метавселенной, меняют свое имущественное и финансовое положение и в реальности, расширяют свой бизнес или получают новые услуги в метамире.

Определяя метавселенную как место исполнения обязательства, остановимся на следующих спорных вопросах – можно ли в принципе определить ее как место для реального мира? И как определить в договоре или законе данное место исполнения обязательства?

Концептуально можно определить метавселенную исключительно как искусственное явление, не более чем игровое пространство и тогда местом исполнения

обязательства опять, как и в реальных сделках, будет признана юрисдикция компании-правообладателя на данную метавселенную. Специфики самой метавселенной как места исполнения обязательства, указано не будет, только в привязке, например, с правами пользования (соглашение по использованию игрового аватара, артефактов и т. д. в конкретной игре или на конкретной платформе).

Альтернативно, реальный мир (государство в рамках конкретных нормативных правовых актов) может признавать отдельный статус метавселенных и правовую связь между обоими мирами (реальным и виртуальным). В такой ситуации метавселенная в какой-то степени станет продолжением реального мира и получит виртуально полноценные адреса (метавселенная, город, адрес – улица, дом, метадом [4. С. 33-42]). То есть при заключении договора и при его исполнении местом будет указана именно сама метавселенная и конкретно адрес в ней.

Метавселенная по своему назначению может быть использована для развития сферы социальных сетей, компьютерных игр, отношений с криптовалютой, удаленной работы и т. д. Существует мнение, что, возможно, будет создана метавселенная с назначением разрешения споров между пользователями других метавселенных [1].

Потенциально возможна ситуация, что любая создаваемая метавселенная будет формироваться по принципу полностью самостоятельного отдельного мира со своими законами, финансовой системой (возможно, признаваемой в реальном мире в качестве криптовалюты или иных финансовых прав), органами власти, в том числе и судом. Такой суд сможет рассматривать споры, которые остаются исключительно внутри метавселенной и последствий в реальном мире не создают (для объективности такого суда его можно определить, как искусственный интеллект, а не владелец метавселенной). Внешнее воздействие будет фактически заключаться только в управлении серверами соответствующими компаниями – владельцами или администраторами.

Для развития этого направления государство должно максимально идентифицировать метавселенные как самостоятельный виртуальный мир с его характеристиками и классификацией, определить юридическое значение внутренней администрации метавселенной, ее принципов и правил взаимодействия с пользователями. Конечно, о полном статусе муниципального образования речи иди не может, но, если уже существует полноценный рынок виртуальной недвижимости в метавселенных (метадома или иные объекты виртуальной недвижимости), рынок NFT-токенов в них же, оборот исключительных прав по поводу и внутри метамира – государству необходимо определить их статус и создать условия защиты интересов пользователей и правообладателей в отношении такого имущества и имущественных прав. Отнесение формируемых в метавселенных прав к категории прав, возникающих в рамках игр и пари, считаем концептуально некорректным.

Возвращаясь к нормативному определению метавселенной как места исполнения обязательства, отметим, что на уровне договорного регулирования, особенно если сам договор заключается на платформе метавселенной, место исполнения обязательства, как и место заключения договора, – это выбор самих сторон. В такой ситуации сторонам можно только рекомендовать обязательно указывать

применимое к договору право для избежания дополнительных сложностей при разрешении спорных ситуаций.

Законодательно в ситуации исполнения обязательства по договору в метавселенной необходимо предусмотреть соответствующее уточнение, например, место нахождения виртуального имущества, место нахождения субъекта отношений – электронного субъекта, цифрового субъекта, место возникновения или место реализации исключительных прав или прав по пользовательскому соглашению.

Такое уточнение, в случае отсутствия необходимой информации по месту исполнения обязательства в самом договоре, позволит точно определить, что само обязательство подлежит исполнению в конкретной метавселенной.

Заключение. Подводя итог исследованию метавселенной как места исполнения обязательства, отметим, что государству необходимо качественно пересмотреть подход к нормативному определению виртуального пространства и его отдельных миров. Сейчас регулирование преимущественно сосредоточено на программных документах [2] и отдельных стандартах. Законодательное закрепление определения, классификационных признаков, разновидностей и принципов метавселенных позволит идентифицировать данный объект как конкретное место в виртуальном мире и показать его связь с реальным миром. После внесения соответствующих уточнений определить метавселенную как место исполнения обязательства даже на законодательном уровне не составит труда.

Список литературы

1. Агатеев А., Бузько Р. Юридические аспекты метавселенной. URL: https://www.buzko.legal/content-ru/yuridicheskie-aspekty-metavselennoy

2. Дорожная карта развития «сквозной» цифровой технологии «Технологии виртуальной и дополненной реальности», 10 октября 2019 г. // СПС «КонсультантПлюс».

3. Лескина Э. И. Метавселенная и задачи в области правового регулирования данных // Юрист. 2023. № 3. С. 2-7.

4. Малеина М. Н. Правовой режим зданий и сооружений, не прикрепленных к поверхности земли // Журнал российского права. 2023. № 2. С. 33-42.

5. Смирнов Д. Что нужно чтобы разработать настоящую Метавселенную? URL: https://crypto-markets.ru/obshhaya-analitika/7-komponentov-metavselennoj

6. Что такое Web 3.0, и почему он всем стал нужен. URL: https://habr.com/ru/articles/653533

7. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7-32. EDN LCCOJJ

8. CEEK VR запустила продажу виртуальных земель в метавселенной. URL: https://crypto.ru/ceek-vr-zapustila-prodazhu-virtualnyh-zemel

9. Zhao Ruoyu, Zhang Yushu, Zhu Youwen [et al.]. Metaverse: Security and Privacy Concerns // Journal of latex class files. 2021. Vol. 14, Iss. 8. P. 1-7.

А. И. Хабиров,
кандидат юридических наук, доцент,
Казанский (Приволжский) федеральный университет

ПРАВОВОЙ РЕЖИМ ИНФОРМАЦИИ, РАЗМЕЩЕННОЙ НА САЙТЕ ИНТЕРНЕТ-МАГАЗИНА

Аннотация. В статье рассматриваются проблемы защиты прав потребителя при заключении договора онлайн. Анализируется специфика механизма возникновения договорных правоотношений в сфере электронной коммерции, а именно возможность квалификации информации, размещенной на сайте продавца (исполнителя) в сети Интернет, в качестве оферты, в том числе публичной. Приводится соответствующая судебная практика арбитражных судов и судов общей юрисдикции.

Ключевые слова: электронная коммерция, оферта, публичная оферта, защита прав потребителей, суд, судебная практика

LEGAL REGIME OF INFORMATION POSTED ON THE WEBSITE OF THE ONLINE STORE

Abstract. The author examines the problems of consumer protection when concluding an online contract. The specifics of the emergence of contractual legal relations in the online environment are analyzed, namely, the possibility of qualifying information posted on the seller's (contractor's) website on the Internet as an offer, including public. The relevant judicial practice is given.

Keywords: e-commerce, offer, public offer, consumer protection, court, judition practice

В статье рассматривается вопрос о возможности квалификации информации, размещенной на сайте в сети Интернет, в качестве оферты. Офертой следует признать такое предложение заключить договор, которое включает в себя два основных элемента: 1) наличие всех существенных условий будущего договора (определенность); 2) намерение лица считать себя заключившим договор с тем, кто примет это предложение (волевая направленность). Правильная квалификация наличия обоих элементов важна [7. С. 40], например, при наличии дисклеймера на сайте продавца. Так, в теории [20. С. 75] и на практике вызывает определенные трудности правовая квалификация информации, размещенной на сайте интернет-магазина. У такой информации может быть разный правовой режим: 1) реклама; 2) просто информация; 3) оферта. У каждого из этих видов информации свой правовой режим и свои правовые последствия, и в зависимости от того, как эта информация будет квалифицирована, меняются правовые последствия. Например, если квалифицировать информацию, размещенную на сайте, в качестве оферты (если в ней содержится описание товара, цена), тогда это будет означать, что действия потребителя по ее дальнейшему принятию являются акцептом и тем самым договор уже будет считаться заключенным. После этого договор в одностороннем порядке

можно будет изменить только в очень ограниченном количестве случаев, особенно когда в качестве клиента выступает потребитель. Следовательно, все риски, связанные с тем, что впоследствии этот договор станет невыгодно исполнять с экономической точки зрения, в значительной степени будут лежать на предпринимателе. Например, курс национальной валюты по отношению к зарубежным валютам резко изменится и продавцу придется закупать заказанные у него товары совсем по другой цене. Конечно, в каких-то случаях можно говорить о форс-мажорных обстоятельствах, о существенном изменении обстоятельств, но их наличие сложно доказать, особенно лицам, занимающимся предпринимательской деятельностью, на которых в силу ст. 401 Гражданского кодекса Российской Федерации (далее – ГК РФ) лежит повышенный риск.

Напротив, если квалифицировать информацию, размещенную на сайте, в качестве вызова на оферту, то действия, которые совершает клиент при оформлении заказа, еще не приводят к заключению договора и у владельца сайта, предпринимателя, сохраняются свобода усмотрения и возможность еще раз подумать, а надо ли подтверждать волеизъявление со стороны клиента и заключать с ним договор или нет. Для обеспечения подобного благоприятного режима для владельца сайта зачастую предусматривают так называемые дисклеймеры – оговорки о том, что информация на сайте не является офертой и носит исключительно справочный характер. Насколько эти дисклеймеры действительно полезны на практике? Судебная практика по данному вопросу противоречива и суды по-разному подходят к квалификации правового режима информации на сайте.

Здесь следует сделать оговорку: правовая квалификация информации на сайте во многом зависит от предмета. Так, если речь идет о продаже вещей и, соответственно, заключается договор дистанционной купли-продажи [1. С. 17], то здесь применяются императивные правила ГК РФ, Закона РФ «О защите прав потребителей», Правила розничной продажи № 2463 [23], которые устанавливают обязанность продавца заключить договор с любым лицом, выразившим намерение заключить договор [5. С. 18]. Кроме того, согласно новой редакции п. 2 ст. 494 ГК РФ, в публичной оферте необязательно указывать цену и иные существенные условия договора розничной купли-продажи. Неудивительно, что при анализе судебной практики можно встретить большое количество дел, в которых суды считали, что любая информация на сайте, содержащая условия будущего договора, является офертой. В частности, если вопрос касался заключения договора дистанционной купли-продажи, то суды общей юрисдикции квалифицировали информацию на сайте в качестве оферты, если в ней содержались наименование, количество и цена товара [4, 39–41]. Подобную же практику можно найти в системе арбитражных судов, которые рассматривали вопрос квалификации информации на сайте в контексте возможности привлечения предпринимателей к ответственности по требованию Роспотребнадзора за нарушение прав потребителей при заключении договора [21, 22, 24, 25, 30]. Схожий подход суды применяли не только при признании заключенными договоров купли-продажи товаров, но также и при рассмотрении споров о признании заключенными иных гражданско-правовых договоров, например, договора возмездного оказания курьерских услуг [32],

договора транспортной экспедиции [33]. Также есть и иные обстоятельства, которые позволяют судам квалифицировать информацию на сайте в качестве оферты, например, наличие возможности оплатить товар или услугу на сайте [37, 38].

Однако есть и иная практика, которая предполагает более вдумчивый анализ того, что размещено на сайте [5. С. 19]. Были примеры, когда отсутствие дисклеймера на сайте, напротив, являлось ключевым фактором вывода суда о том, что эта информация являлась офертой, т. е. суды указывали, что, если бы дисклеймер был, информация на сайте не была бы квалифицирована в качестве оферты [15, 28]. Правда, здесь следует заметить, что подобная практика не является системной, повсеместной. Более того, в каком-то смысле она противоречит публичному регулированию, а именно п. 17 Правил розничной продажи товаров, согласно которому при дистанционном способе продажи товара с использованием сети Интернет продавец обязан обеспечить возможность ознакомления потребителя с офертой путем ее размещения на сайте и (или) странице сайта в сети Интернет и (или) в программе для электронных вычислительных машин, если соглашением между продавцом и владельцем агрегатора не предусмотрен иной порядок исполнения такой обязанности. Арбитражные суды при разрешении споров между Роспотребнадзором и продавцом (исполнителем, владельцем агрегатора) также указывают, что отсутствие на сайте текста публичной оферты нарушает право потребителей на получение всей необходимой по закону информации при продаже товаров [27]. В то же время наличие дисклеймера о справочном характере цены и другой размещенной на сайте информации трактуется арбитражными судами в качестве нарушения права потребителя на получение достоверной информации о товаре или услуге [24, 25, 30].

Также, исходя из анализа судебной практики, можно выделить и ряд других обстоятельств, которые могут повлиять на признание информации на сайте не являющейся офертой. Так, если на сайте прямо указывается на необходимость согласования условий продажи и доставки с менеджерами компании, отсутствуют необходимые реквизиты продавца по договору реализации товара в розницу, а также условия о сроках исполнения договора, порядке его оплаты при доставке в другие регионы транспортной компанией, то размещенная на сайте информация о возможности приобретения (поставки, изготовления) товара не отвечает понятию публичной оферты розничного договора купли-продажи. Напротив, такая информация представляет собой лишь приглашение делать оферты [21]. Также суды указывают, что если на сайте размещен баннер «сообщить о поступлении» [29], есть возможность зарезервировать товар (онлайн-бронирование) без оплаты [19, 34] либо отсутствует существенное условие [12, 34, 42], то информация на сайте будет квалифицирована как реклама, т. е. лишь предложение делать оферты. Следует отдельно остановиться на последнем примере (отсутствии существенного условия) и приведенной судебной практики. Дело в том, что все приведенные примеры из судебной практики касаются продажи автомобилей. Суды при анализе информации, размещенной на сайте автосалонов, единогласно не признают ее офертой, даже несмотря на то, что, как правило, указываются данные о предмете (марка и модель машины), стоимость соответствующей комплектации. В ка-

честве обоснования подобного подхода в судебных решениях фигурирует ссылка на несогласование предмета будущего договора в связи с тем, что отсутствует вин-номер конкретного автомобиля, а значит, по мнению судов, невозможно достоверно определить, какой именно автомобиль подлежит передаче покупателю. Представляется, что подобная аргументация не выдерживает критики, поскольку при продаже иных технически сложных товаров – телефонов, ноутбуков и т. п. (а автомобиль тоже отнесен к числу таких товаров), – суды не требуют указывать номер конкретного устройства, которое в дальнейшем будет продано покупателю. А ведь у каждого подобного устройства (телефон, ноутбук и т. д.) есть свой индивидуальный номер.

Кроме того, согласно ст. 494 ГК РФ и пункту 16 Правил розничной продажи № 2463, продавец имеет право отказать в заключении договора, если товар не предназначен для продажи. Это правило активно используется участниками рынка для того, чтобы избежать удовлетворения требования потребителя о признании договора заключенным и о передаче товара. Сама формулировка, использованная в указанных нормативных правовых актах, предоставляет большой простор для фантазии при ее реализации. В частности, некоторые продавцы разработали свои собственные правила продажи товаров, например, Правила «Wildberries» о технически сложных товарах, в которых прямо указывается, что любой технически сложный товар не предназначен для продажи дистанционным способом. Данное правило уже само по себе противоречит логике, так как указанный продавец реализует товары только дистанционным способом. Неудивительно, что суды также подтвердили, что одного указания продавцом на «непредназначенность» товара для дистанционной продажи недостаточно [2, 17, 35]. Более того, согласно устоявшейся судебной практике сам по себе факт оформления заказа, присвоения ему номера, подтверждения оплаты товара и сообщения места и времени его выдачи свидетельствует о заключении договора купли-продажи между истцом и ответчиком дистанционным способом. Если товар доступен для покупки, продавец таким образом гарантирует его наличие, а значит, и предназначенность для продажи дистанционным способом [37]. И, напротив, указание на определенную аудиторию покупателей может быть истолковано как конкретизация непредназначенности товара для дистанционной продажи (т. е. для всех). Пример из судебной практики – продажа устройств нагревания табака [36].

И, наконец, в контексте квалификации информации на сайте в качестве оферты следует рассмотреть вопрос о влиянии технического сбоя на статус уже заключенного договора. Как в отечественной, так и в зарубежной практике периодически имеют место ошибки, допускаемые продавцом, исполнителем, владельцем агрегатора [9. С. 150], при размещении информации о продаваемых товарах на сайте. Наибольший резонанс вызывают ошибки при указании цены продаваемого товара, программного обеспечения или услуг. Зачастую об этих ошибках становится известно уже после того, как потребитель успевает заказать и оплатить товар. Возникает вопрос о юридической судьбе заключенного договора. Имеет ли в таком случае продавец право отказаться от договора в одностороннем порядке? Исходя из имеющейся судебной и иной правоприменительной практики, однозначный от-

вет на данный вопрос отсутствует. В Правилах розничной продажи указывается, что при продажах через Интернет договор розничной купли-продажи считается заключенным с момента выдачи продавцом потребителю кассового или товарного чека либо иного документа, подтверждающего оплату товара, или с момента получения продавцом сообщения потребителя о намерении заключить договор розничной купли-продажи. На это же обращает внимание и Роспотребнадзор, указывая, что норм, предусматривающих возможность расторгнуть такой договор, Правила продажи не предусматривают. Кроме того, потребитель вполне мог счесть данную ценовую политику способом привлечения внимания к тому или иному товару или бренду, в том числе и в случаях, когда товар продается за один рубль, что является распространенной практикой привлечения внимания к тому или иному товару или бренду [10]. Также имеется соответствующая практика, когда суды констатируют, что технический сбой у интернет-магазина не может быть отнесен к исключающим вину продавца обстоятельствам, поскольку у продавца имелась возможность для соблюдения правил и норм, за нарушение которых предусмотрена административная ответственность, но им не были приняты все зависящие от него меры по их соблюдению. Суд полагает, что технические сбои (отключения/повреждения электропитания и сетей связи, сбоев программного обеспечения) не относятся к обстоятельствам непреодолимой силы, исключающим ответственность за неисполнение обязательств [18, 26, 31]. Более того, даже если товар был продан по цене, существенно ниже рыночной, суды удовлетворяют требования потребителя о признании договора заключенным и о передаче товара. В одном из дел суд констатировал следующее: «Ответчик указал все существенные условия договора – индивидуализировал товар, указал его стоимость и порядок приобретения. При этом заявка была принята и зарегистрирована. Факт отсутствия товара на складе у продавца не имеет правового значения для разрешения настоящего спора, поскольку из материалов дела следует, что указанный товар с производства не снят, его поставки не прекращены. Размещенная на сайте ответчика информация о товаре достаточна для ее квалификации в качестве оферты, которая была акцептована потребителем посредством размещения заказа. Ссылку ответчика на отсутствие у информации на сайте статуса публичной оферты суд не принимает во внимание, поскольку сделанные продавцом оговорки, по мнению суда, преследуют цель сохранения за собой контроля над моментом заключения договора. Доводы ответчика о сбое на сайте компании, в результате которого стоимость куттера, указанная на сайте, значительно ниже реальной стоимости товара, не имеет значения для существа рассматриваемого дела, поскольку данное обстоятельство суд расценивает как риск предпринимательской деятельности в совокупности с ответственностью должника за действия своих работников» [42].

Однако есть и иная трактовка судами данных обстоятельств. В частности, суды констатируют, что очевидность факта технического сбоя для потребителя влечет невозможность принудительного исполнения договора по его требованию. Так, в одном из определений суд указал, что потребитель был проинформирован о происшедшем техническом сбое на веб-сайте и невозможности заключения договора по цене, указанной на веб-сайте, незамедлительно после получения соот-

ветствующего сообщения потребителя. Суд отметил, что требование потребителя об исполнении договора по такой цене со ссылками на нормы об оферте и акцепте являлось злоупотреблением правом [13, 16]. Либо суды констатируют, что при заявлении продавцом о произошедшем сбое стороны не достигли соглашения по цене, следовательно, договор следует считать незаключенным [3, 11].

Подводя итоги проведенного исследования, следует выделить следующее.

Во-первых, исходя из анализа юридической доктрины, фактически складывающихся отношений между участниками оборота и судебной практики, необходимо подчеркнуть важность и актуальность исследования вопроса о механизме заключения договора дистанционным способом, в том числе правильной квалификации информации, размещенной на сайте продавца, изготовителя, агрегатора.

Во-вторых, следует отметить отсутствие единообразия судебной практики по вопросу квалификации рассматриваемой информации, причем это касается как арбитражных судов, так и судов общей юрисдикции. В схожих ситуациях суды по-разному квалифицируют информацию на сайте и, как следствие, это влияет на квалификацию сложившихся между сторонами отношений.

В-третьих, в связи с изложенным представляется необходимым провести обобщение имеющейся судебной практики по исследуемому вопросу в целях единообразного толкования судами норм ГК РФ, закона РФ «О защите прав потребителей» и Правил розничной продажи.

Список литературы

1. Андреева Л. В. Элементы цифровых технологий в торговой и закупочной деятельности (правовой аспект) // Предпринимательское право. Приложение «Право и Бизнес». 2019. № 1. С. 15-21.

2. Апелляционное определение Зеленоградского районного суда Калининградской области от 27.12.2021 по делу № 11-16/2021 // СПС «Консультант Плюс».

3. Апелляционное определение Московского городского суда 20 июля 2022 года по делу № 33-27492/2022 // СПС «Консультант Плюс».

4. Апелляционное определение Санкт-Петербургского городского суда № 33-12497/2022 по делу № 2-7760/2021 от 28.07.2022 // СПС «Консультант Плюс».

5. Белов В. А. Смарт-торговля (цифровая торговля): основные положения о цифровизации договорных отношений с участием потребителей // Вестник арбитражной практики. 2022. № 3. С. 17-23.

6. Белов В. А. Электронная торговля: понятие, правовое регулирование и судебная практика // Вестник арбитражной практики. 2021. № 4. С. 11-20.

7. Демченко М. В., Шайдуллина В. К. Правовое регулирование электронной торговли в условиях функционирования специальных правовых режимов // Предпринимательское право. 2020. № 3. С. 37-45.

8. Ефимова Л. Г. Понятие и правовые особенности электронного договора // Законы России: опыт, анализ, практика. 2019. № 7. С. 84-90.

9. Кузнецова Л. В. Вопросы гражданско-правовой ответственности агрегаторов электронной коммерции // E-commerce и взаимосвязанные области (правовое регулирование): сборник статей / А. А. Богустов, О. Н. Горохова, Д. А. Доротенко и др.; рук. авт. кол. и отв. ред. М. А. Рожкова. М.: Статут, 2019. 448 с.

10. О недобросовестной практике маркетинговых акций отдельных компаний. URL: https://www.rospotrebnadzor.ru

11. Определение Восьмого кассационного суда общей юрисдикции от 28.04.2021 по делу № 88-7517/2021 // СПС «Консультант Плюс».

12. Определение Московского городского суда от 18.10.2021 по делу № 33-27316/2021 // СПС «Консультант Плюс».

13. Определение Первого кассационного суда общей юрисдикции от 07.04.2021 № 88-6481/2021 // СПС «Консультант Плюс».

14. Определение Первого кассационного суда общей юрисдикции от 19.11.2020 по делу № 88-24114/2020 // СПС «Консультант Плюс».

15. Определение Четвертого кассационного суда общей юрисдикции от 20.10.2020 по делу № 88-20176/2020 // СПС «Консультант Плюс».

16. Определение Шестого кассационного суда общей юрисдикции от 08.02.2022 по делу № 8Г-357/2022-(8Г-30152/2021) // СПС «Консультант Плюс».

17. Определение Шестого кассационного суда общей юрисдикции от 09.08.2022 № 88-14758/2022 по делу № 2-4707/2021 // СПС «Консультант Плюс». 18. Определение Шестого кассационного суда общей юрисдикции от 15.03.2022 по делу № 88-5725/2022 // СПС «Консультант Плюс».

19. Определение Шестого кассационного суда общей юрисдикции от 16.08.2022 № 88-16245/2022 по делу № 2-186/2022 // СПС «Консультант Плюс».

20. Останина Е. А. Публичный договор, заключаемый онлайн, и защита прав потребителя // Имущественные отношения в Российской Федерации. 2019. № 8. С. 67-75.

21. Постановление Десятого арбитражного апелляционного суда от 20.08.2019 № 10АП-13477/2019 по делу № А41-6122/2019 // СПС «Консультант Плюс».

22. Постановление Первого арбитражного апелляционного суда от 13.11.2018 по делу № А43-30888/2018 // СПС «Консультант Плюс».

23. Постановление Правительства РФ от 31.12.2020 № 2463 «Об утверждении Правил продажи товаров по договору розничной купли-продажи, перечня товаров длительного пользования, на которые не распространяется требование потребителя о безвозмездном предоставлении ему товара, обладающего этими же основными потребительскими свойствами, на период ремонта или замены такого товара, и перечня непродовольственных товаров надлежащего качества, не подлежащих обмену, а также о внесении изменений в некоторые акты Правительства Российской Федерации» // Собрание законодательства РФ. 2021. № 3. Ст. 593.

24. Постановление Семнадцатого арбитражного апелляционного суда от 24.12.2021 № 17АП-14695/2021-АК по делу № А60-35541/2021 // СПС «Консультант Плюс».

25. Постановление Семнадцатого арбитражного апелляционного суда от 27 июня 2022 г. № 17АП-4622/22 по делу № А60-321/2022 // СПС «Консультант Плюс».

26. Решение арбитражного суда Астраханской области от 3 сентября 2021 года по делу № А06-4221/2021 // СПС «Консультант Плюс».

27. Решение Арбитражного суда г. Москвы от 07.10.2021 по делу № А40-158993 // СПС «Консультант Плюс».

28. Решение Арбитражного суда города Санкт-Петербурга и Ленинградской области от 8 ноября 2018 г. делу № А56-99176/2018 // СПС «Консультант Плюс».

29. Решение Арбитражного суда города Санкт-Петербурга и Ленинградской области от 14 мая 2021 г. по делу № А56-3002/2021 // СПС «Консультант Плюс».

30. Решение Арбитражного суда Хабаровского края от 3 сентября 2021 г. по делу № А06-4221/2021 // СПС «Консультант Плюс».

31. Решение АС Республики Татарстан от 20 сентября 2021 г. по делу № А65-11431/2021 // СПС «Консультант Плюс».

32. Решение Благовещенского городского суда Амурской области от 17 сентября 2020 г. по делу № 2-3766/2020 // СПС «Консультант Плюс».

33. Решение Каменского районного суда Ростовской области от 6 июля 2020 г. по делу № 2-512/2020 // СПС «Консультант Плюс».

34. Решение Кировского районного суда города Хабаровска от 19.02.2021 по делу № 2-263/2021 // СПС «Консультант Плюс».

35. Решение Костромского районного суда Костромской области от 10.08.2022 по делу № 2-770/2022 // СПС «Консультант Плюс».

36. Решение Мотовилихинского районного суда г. Перми от 19.07.2022 // СПС «Консультант Плюс».

37. Решение Октябрьского районного суда города Белгорода от 28.05.2021 по делу № 2-3083/2021 // СПС «Консультант Плюс».

38. Решение Пригородного районного суда Свердловской области от 15 января 2019 г. по делу № 2-68/2019 // СПС «Консультант Плюс».

39. Решение Промышленного районного суда г. Смоленска от 30 апреля 2015 по делу № 2-2013/2015 // СПС «Консультант Плюс».

40. Решение Саратовского районного суда Саратовской области от 16.11.2021 по делу № 2-1036/2021 // СПС «Консультант Плюс».

41. Решение Свердловского районного суда города Белгорода от 07.04.2021 № 552-708/2021 // СПС «Консультант Плюс».

42. Решение Советского районного суда г. Воронежа от 3 июля 2022 по делу № 2-741\2020 // СПС «Консультант Плюс».

43. Решение Щелковского городского суда Московской области от 30.05.2022 по делу № 2-2749/2022 // СПС «Консультант Плюс».

44. Решение Щелковского районного суда от 30 мая 2022 г. по делу № 2-2749/2022 // СПС «Консультант Плюс».

Е. В. Хамидуллина,
ассистент,
Санкт-Петербургский государственный экономический университет

ПРАВОВАЯ ПРИРОДА УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ, ПРИНЯТЫХ ИСКУССТВЕННЫМ ИНТЕЛЛЕКТОМ

Аннотация. Основной целью исследования является теоретическое осмысление тенденций использования технологий искусственного интеллекта в корпоративных правоотношениях. Выбор темы обусловлен наличием дискуссионных вопросов в отношении правового режима искусственного интеллекта. В статье произведен анализ сфер корпоративного управления, в которых происходит активное внедрение искусственного интеллекта. Сформулирован вывод о необходимости отражения последних тенденций деятельности корпораций в действующем законодательстве. Рассмотрены варианты в отношении места искусственного интеллекта в корпоративном праве.

Ключевые слова: искусственный интеллект, корпоративное право, большие данные, управление, ответственность, субъект права, объект права

LEGAL NATURE OF MANAGEMENT DECISIONS MADE BY ARTIFICIAL INTELLIGENCE

Abstract. The main goal of the study is a theoretical understanding of trends in the use of artificial intelligence technologies in corporate legal relations. The choice of topic is due to the presence of controversial issues regarding the legal regime of artificial intelligence. The article analyzes the areas of corporate governance in which artificial intelligence is being actively implemented. The conclusion is formulated about the need to reflect the latest trends in the activities of corporations in the current legislation. Options regarding the place of artificial intelligence in corporate law are considered.

Keywords: artificial intelligence, corporate law, big data, management, responsibility, subject of law, object of law

В современном мире искусственный интеллект способен не только решать сложные вычислительные задачи, но и справляется с имитацией когнитивных функций человека. Технологии искусственного интеллекта принято делить на два класса: сильный и слабый. К сильному искусственному интеллекту относят технологии, которые могут самообучаться и осуществляют деятельность, сопоставимую с человеческой деятельностью. К слабому искусственному интеллекту относят технологии, которые выполняют ограниченное количество функций, например, поиск и воспроизведение музыкальных произведений, осуществление поисковых запросов, распознавание речи. Приведенная классификация является условной и не закреплена в российских нормативных правовых актах.

На постоянной основе ведутся многочисленные дискуссии относительно возможности замены представителей различных профессий на искусственный интеллект. Это связано с возможностью систематизировать различные виды дея-

тельности. Искусственный интеллект уже привлекается для проверки письменных работ. Предполагается, что он способен осуществлять преподавание – проводить занятия и проверять знания студентов. Технологии искусственного интеллекта активно используются в сфере искусства. С их помощью создаются картины, пишутся стихи и проза, генерируются музыкальные произведения. В перспективе предполагается, что искусственный интеллект сможет составлять исковые заявления и даже выносить решения вместо судьи. Даже такая важная сфера, как медицина, не осталась без внимания разработчиков искусственного интеллекта. При помощи него ставится диагноз и назначается лечение на основе жалоб пациента и результатов его анализов.

Существует прецедент сдачи искусственным интеллектом экзамена для адвокатов [3]. Несмотря на то, что экзаменаторы поставили нейросети ChatGPT высокие баллы, ответ содержал некоторые неточности. При ответе на один из вопросов ChatGPT не делал ссылки на нормативные правовые акты и давал обобщенную информацию. При ответе на другой вопрос он сделал ссылку на закон, но указал статью неправильно. В целом его ответы содержали некоторую путаницу в юридической терминологии и отсутствие понимания сути некоторых поставленных вопросов. Как отмечает автор статьи, искусственный интеллект показал «школьный» уровень знаний. Неудивительно, что искусственный интеллект нашел применение в такой подотрасли как корпоративное право.

Если отойти от восприятия искусственного интеллекта как полной замены человека, то его можно рассматривать как средство оптимизации работы организации. Прежде всего искусственный интеллект можно использовать при обработке большого объема информации. На основе анализа электронных документов он способен в короткие сроки произвести классификацию и структурировать их. Таким образом происходит автоматизация работы с электронными документами. Искусственный интеллект способен собирать колоссальные массивы данных, которые охватить «вручную» невозможно [6]. Помимо быстрого поиска необходимой информации, искусственный интеллект позволяет отслеживать тенденции изменения в различных сферах деятельности корпоративных юридических лиц и предлагать оптимально выгодные условия для развития. В качестве плюсов работы с информацией при помощи искусственного интеллекта можно выделить скорость обработки больших массивов данных и отсутствие «человеческого фактора.

На основе внутренней и внешней информации искусственный интеллект способен составлять прогнозы по различным направлениям деятельности корпорации. Он может произвести анализ данных для определения оптимальной цены, обозначить круг потенциальных потребителей и предложить план для привлечения новых. Новшеством является поиск сотрудников на основе анализа искусственным интеллектом резюме претендентов.

Исследователи выделяют три типа цифрового управления в корпорации:

– дистанционное управление, которое осуществляется непосредственно человеком;

– смарт-управление, которое производится при помощи заранее заданного алгоритма;

– управление искусственным интеллектом [4].

Особенностью управления корпорацией при помощи искусственного интеллекта является отсутствие заранее заложенных в программе решений [2]. В качестве преимущества данного подхода выделяют скорость принятия решений, отсутствие эмоциональной составляющей и способность к обработке большого объема данных. Искусственный интеллект способен не только самостоятельно принимать решения, но и взаимодействовать с человеком, например, оценивать риски при одобрении членами совета директоров стратегически важных сделок. Голосование членов совета директоров может длиться до совпадения их мнения с выводами искусственного интеллекта. Технологии искусственного интеллекта также применяются при подборе персонала на этапах рутинной работы по отбору резюме, адаптации сотрудников, оценки их качества работы и повышения квалификации.

Под управленческим решением в корпорации понимается результат, который разрабатывается и реализуется для разнородной социальной системы с многоуровневой системой управления и направлен на формирование и поддержание функционирования организационных механизмов, способствующих гармонизации отношений в корпорации, а также на обеспечение стабильности структуры ресурсов корпорации [7]. В процессе управления корпорацией при помощи искусственного интеллекта можно столкнуться с проблемой возложения ответственности за качество прогнозов искусственного интеллекта. В пп. а п. 5 Указа Президента РФ от 10.10.2019 № 490 и п. 2 ст. 2 Федерального закона от 24.04.2020 № 123-ФЗ искусственный интеллект определяется как объект права. В корпоративных правоотношениях он является техническим ресурсом корпорации. Разумеется, ответственность за принятие управленческих решений можно возложить только на субъект права. Исследователи выделяют различные предложения, согласно которым искусственный интеллект следует наделить правосубъектностью [1, 7], но с учетом правового регулирования искусственного интеллекта в Российской Федерации и уровня развития технологий искусственного интеллекта на современном этапе подобные изменения законодательства не представляются целесообразными.

Согласно ст. 65.3 Гражданского кодекса Российской Федерации управленческие решения в корпорации могут приниматься высшим исполнительным органом корпорации, единоличным исполнительным органом корпорации и коллегиальным органом управления корпорацией. В практике иностранных государств (Китай, США и др.) можно встретить наблюдательные советы по учету информационных технологий, которые несут ответственность за принимаемые искусственным интеллектом решения [5]. Так как искусственный интеллект не может являться участником корпорации, возникает вопрос о законности генерируемых им решений. В ситуации, когда искусственный интеллект разрабатывает основу (проводит анализ данных) для управленческих решений органов корпорации, ответственность за последствия таких решений следует возлагать на органы, их принимающие. Это связано с фактическим участием органов корпорации в осу-

ществлении управления. Можно ли говорить о подобном волеизъявлении, если уровень автономности искусственного интеллекта является высоким, и решения принимаются автоматически, без их оценки участниками корпорации? Здесь можно провести параллель с интуитивным управлением, когда принимаемые решения не основываются на рациональном подходе, а обуславливаются опытом и квалификацией участников.

Искусственный интеллект неспособен нести ответственность за генерируемые решения, ее представляется возможным возложить на участников корпорации, которые одобряют их (активными действиями или бездействием) или на создателя искусственного интеллекта [5]. В данной ситуации многое зависит от гарантий создателя искусственного интеллекта. Сложно себе представить, чтобы он обещал корпорациям безошибочность решений, принимаемых искусственным интеллектом [8]. Таким образом, основываясь на контролирующем характере управленческой деятельности, ответственность за решения, принимаемые искусственным интеллектом, следует возлагать на субъекты корпоративных правоотношений в соответствии с действующим законодательством.

Список литературы

1. Бегишев И. Р. Искусственный интеллект и робот как правовые категории // Безопасность бизнеса. 2020. № 6. С. 32-36. EDN FNITTF.

2. Галлезе-Нобиле К. Регулирование умных роботов и искусственного интеллекта в Европейском союзе // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 33-61. EDN UNSONV

3. Ефременко Е. Как нейросеть ChatGPT сдавала экзамен на адвоката и писала юридические заключения. URL: https://pravo.ru/story/245248

4. Лаптев В. А., Чуча С. Ю., Фейзрахманова, Д. Р. Цифровая трансформация инструментов управления современными корпорациями: состояние и пути развития // Правоприменение. 2022. № 1. С. 229-244.

5. Панабергенова Ж. Т. Правовые аспекты применения искусственного интеллекта в корпоративном управлении// Universum: экономика и юриспруденция. 2023. № 4(103). С. 16-18.

6. Сулимов Н. Ю. Внедрение искусственного интеллекта в систему корпоративного управления // Инновации и инвестиции. 2023. № 7. С. 136-139.

7. Филипова И. А., Коротеев В. Д. Будущее искусственного интеллекта: объект или субъект права? // Journal of Digital Technologies and Law. 2023. Т. 1, № 2. С. 359-386. EDN IMMOAM.

8. Юсупова С. М., Алавина Е. М. Особенности принятия управленческих решений в корпорациях // Гуманитарный научный журнал. 2022. № 4-2. С. 48-59.

Е. Г. Шаблова,
доктор юридических наук, профессор,
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина
Н. В. Городнова,
доктор экономических наук, доцент,
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина
О. В. Жевняк,
кандидат юридических наук, доцент,
Уральский федеральный университет
имени первого Президента России Б. Н. Ельцина

ВЫЯВЛЕНИЕ ЧАСТНО-ПРАВОВЫХ ВОПРОСОВ ПРОМЫШЛЕННОГО ИНТЕРНЕТА ВЕЩЕЙ НА ОСНОВЕ ЕГО ТЕХНОЛОГИЧЕСКИХ И ЭКОНОМИЧЕСКИХ ХАРАКТЕРИСТИК

Аннотация. Статья посвящена определению круга частноправовых вопросов промышленного интернета вещей на основе его технологических и экономических характеристик. Рассматривается экономическое значение промышленного интернета вещей и оцениваются перспективы его применения в России, анализируются технологические характеристики промышленного интернета вещей и бизнес-модели, применяемые при его коммерческом внедрении, имеющие частно-правовое значение, на основе этого выявляются вопросы, связанные с промышленным интернетом вещей, входящие в предмет частного права. Научной новизной отличается выявление технологических характеристик промышленного интернета вещей, которые имеют частноправовое значение, построение системы гражданско-правовых договоров в зависимости от их роли в обеспечении функционирования промышленного интернета вещей, моделирование IIoT-зрелости российских компаний, развитие алгоритма принятия IIoT-решений российскими компаниями.

Ключевые слова: промышленный интернет вещей, интернет вещей, IoT, IIoT, правовой режим интернета вещей, правовое регулирование интернета вещей, частноправовое регулирование интернета вещей, договоры в IoT, объекты гражданских прав в IoT, IIoT-зрелость, IIoT-решения

IDENTIFICATION OF PRIVATE LEGAL ISSUES OF THE INDUSTRIAL INTERNET OF THINGS BASED ON ITS TECHNOLOGICAL AND ECONOMIC CHARACTERISTICS

Abstract. The article is devoted to determining the range of private legal issues of the Industrial Internet of Things based on its technological and economic characteristics. The economic significance of the Industrial Internet of Things is considered and the prospects for its use in Russia are assessed. The technological characteristics of the Industrial Internet of Things and the business models used in its commercial implemen-

tation, which have private legal significance, are analyzed. Based on this, issues related to the Industrial Internet of Things are identified that are subject of private law. The scientific novelty is the identification of the technological characteristics of the Industrial Internet of Things that are of private legal significance, the construction of a system of civil law contracts depending on their role in ensuring the functioning of the Industrial Internet of Things, the modeling of the IIoT maturity of Russian companies, the development of an algorithm for making IIoT decisions by Russian companies.

Keywords: Industrial Internet of Things, Internet of Things, IoT, IIoT, IoT legal regime, IoT legal regulation, IoT private law regulation, contracts in IoT, objects of civil rights in IoT, IIoT-maturity, IIoT- decisions

Введение. Применение новых сквозных цифровых технологий (алгоритмы искусственного интеллекта, автономная робототехника, интернет вещей, создание Big Data), а также рост объемов финансирования научно-технических разработок в обозначенной сфере являются магистральным трендом развития российской экономики в России на ближайшее десятилетие. В этой связи тема исследования является, бесспорно, актуальной.

В публикациях встречаются различные определения интернета вещей (Internet of Things, IoT), делающие акценты на различных его особенностях [23, 29, 30, 34, 36]. Предлагаем следующее описание интернета вещей – это технология, которая позволяет объединить в единую взаимосвязанную систему множество устройств (приборов, сенсоров и датчиков) и компьютерных программ, при этом устройства представляют собой физические объекты с программным обеспечением, которые систематически считывают информацию о физических объектах, явлениях и процессах, передают эту информацию в режиме реального времени по каналам электросвязи для автоматической обработки компьютерными программами, результаты анализа большого объема информации становятся основой для принятия автоматических (или с участием человека) решений по управлению физическими объектами, процессами, явлениями; принятые решения передаются через каналы электросвязи и исполняются автоматически помощью компьютерных программ (или с участием человека).

IoT относят к киберфизическим системам, которые являются системами управления данными, включающими в себя определенную степень интеллекта и работающими в реальном времени, чтобы влиять на результаты в реальном мире; взаимодействие с физическим миром осуществляется через датчики, обнаруживающие и измеряющие физические параметры для управления физическими процессами [35]. В его функционировании проявляются тенденции слияния технологий и стирания границ между физической и цифровой реальностями, что характерно для четвертой промышленной революции [40].

Выделяют потребительский (CIoT, Consumer Internet of Things) и промышленный интернет вещей (IIoT, Industrial Internet of Things). Последний предназначен «для корпоративного/отраслевого применения» [36], т. е. используется в промышленности, сельском хозяйстве, сфере услуг. При этом устройства, в него входящие, имеют небытовое (как в потребительском интернете вещей) назначе-

ние. IIoT является, по сути, системой управления производством, которая более эффективна по сравнению с традиционной, т. к. предоставляет кардинально иные аналитические возможности, увеличивает скорость принятия управленческих решений, исключает лишние звенья из этого процесса, сокращает ошибки, связанные с включенностью человеческого фактора в процессы производства, экономит ресурсы, снижает затраты, дает возможность применять оборудование и работать сотрудникам удаленно.

В 2023 г. Правительство РФ утвердило дорожную карту по развитию индустриального программного обеспечения, согласно которой в промышленный интернет вещей планируется вложить 90 млрд руб. до 2030 г., а объем рынка отечественных решений на базе технологии IIoT, по прогнозам, должен достигнуть 147,25 млрд руб. против 79,6 млрд рублей в 2022 г. Доля рынка отечественных индустриальных решений будет расти в связи с уходом с рынка западных вендоров и к 2030 г. должна составить 82,74 % (в 2022-м она была 54,1 %). К 2023 г. должна появиться отечественная IIoT-платформа на основе больших данных для управления производством в сельском хозяйстве, добыче полезных ископаемых, промышленности, энергетике, ЖКХ, строительстве, образовании, транспорте и логистике [37].

Состояние научной разработки темы исследования

В одной из предыдущих работ авторами был исследован IIoT как правовая категория, были выявлены его особенности, имеющие юридическое значение, и разработаны идеи для концепции правового регулирования IIoT на федеральном уровне [32]. В другой работе предметом рассмотрения стало региональное регулирование IIoT на примере Свердловской области, где было проанализировано текущее состояние регулирования и разработаны некоторые рекомендации и меры по оценке эффективности внедрения этих рекомендаций [31].

Настоящая статья основывается на следующих научных гипотезах:

1) технологические и экономические характеристики промышленного интернета вещей имеют частноправовое значение;

2) правовой режим промышленного интернета вещей включает не только правила публично-правового характера (направленные на техническое регулирование, обеспечение информационной безопасности, защиту прав работников, вовлеченных в процесс управления производством и др.), но и частноправового характера;

3) предложенные авторами ранее подходы к правовому пониманию интернета вещей вытекают из его технологических и экономических характеристик.

Следует отметить, что в правовой науке в основном исследуются публично-правовые аспекты, причем применительно к интернету вещей в целом (безотносительно промышленного интернета вещей). См., например [1, 4, 5, 8, 10, 22, 28]. Необходимость системного подхода в анализе правового регулирования интернета вещей отмечается в юридической литературе [9, 13, 19]. Однако комплексному исследованию частно-правового регулирования интернета вещей и промышленного интернета вещей не уделяется должного внимания. Авторы акцентируют свое внимание на отдельных вопросах частноправового регулирования: исследу-

ется правовая охрана интеллектуальной собственности [27], проблемы договорного права [24], регулирование качества товара [3, 11], такой предмет сделок, как информация [14], отнесение цифровых данных к объектам гражданских прав [15].

Цель, задачи, методология и новизна исследования

Целью настоящей работы является выявление частноправовых вопросов промышленного интернета вещей на основе анализа технологических и экономических особенностей промышленного интернета вещей.

Для этого решены следующие задачи:

1) проведен анализ экономического значения промышленного интернета вещей и дана оценка перспектив его использования в России;

2) дан анализ технологических характеристик промышленного интернета вещей и бизнес-моделей, используемых при его коммерческом внедрении, которые могут иметь частноправовое значение;

3) выявлен круг частноправовых вопросов промышленного интернета вещей на основе его технологических и экономических характеристик.

Методы исследования: сравнение, описание, анализ и синтез, системный метод, метод экономического анализа, метод моделирования.

Научной новизной обладают следующие положения:

1) выявлены технологические характеристики промышленного интернета вещей, которые имеют частноправовое значение;

2) построена система гражданско-правовых договоров в зависимости от их роли в обеспечении функционирования промышленного интернета вещей;

3) смоделирована IIoT-зрелость российских компаний, развит алгоритм принятия IIoT-решений российских компаний, учтен при этом фактор цифровой трансформации в принятой Правительством России методике оценки «цифровой зрелости».

Основная часть

1. Экономическое значение промышленного интернета вещей

Концепция промышленного интернета вещей заключается в применении вычислительных сетей физических объектов (вещей), оснащенных интегрированными информационными технологиями в целях постоянного и эффективного взаимодействия между собой и с внешней средой.

К ключевым принципам интернета вещей следует отнести:

1) возможность удаленного использования различного оборудования, в том числе в удаленных и недоступных для человека местах и сферах;

2) существенная экономия ресурсов и электроэнергии;

3) сбор, обработка, хранение и использование гигантских массивов информации и данных, позволяющих сократить труд человека и являющихся основой для обучения алгоритмов искусственного интеллекта.

К ключевым принципам реализации идеи промышленного интернета вещей отнесем:

1) сбор информации с различных датчиков, устройств и сенсоров;

2) передача информации между интегрированными устройствами и на главный сервер;

3) система хранения данных и информации, визуализация в понятной для человека форме;

4) процесс принятия решений при помощи алгоритмов искусственного интеллекта.

Основными трендами развития интернета вещей и промышленного интернета вещей на ближайшую перспективу являются:

1) колоссальный рост объемов и скорости передачи информации;

2) создание новых IT-объектов хранения данных, развитие «облачных» технологий и вычислений;

3) развитие системы кибернетической безопасности как одного аспекта надежности решений в сфере интернета вещей;

4) сегментирование единой исходной информации и данных в интересах различных потребителей и пользователей.

Основными позитивными последствиями развития IIoT-технологий являются [25, 26]:

1) постоянный мониторинг информационных потоков в сети Интернет;

2) оценка эффективности рекламных и маркетинговых кампаний;

3) постоянный мониторинг активности компаний-конкурентов;

4) применение алгоритмов искусственного интеллекта;

5) постоянный поиск клиентов и потребителей продукции [16];

6) обеспечение прозрачности осуществления инвестиций для компании.

К фундаментальным факторам роста рынка промышленного интернета вещей авторы относят перспективы тотального внедрения Интернета во всех сферах жизнедеятельности российского общества, развитие мобильных сетей, государственную поддержку IT-сектора, систему комплексной кибернетической безопасности реального и виртуального сегментов российской экономики [21]. Серьезными факторами сдерживания цифровой трансформации являются антироссийские санкции, нестабильность финансово-экономических условий, негативное влияние на экологию, недостаток IT-специалистов и пр.

Идея IIoT направлена на повышение эффективности экономики путем внедрения систем автоматизации всех технологических и общественных процессов. Промышленный интернет вещей как сектор глобального интернета вещей является неотъемлемой частью роста эффективности российской экономики [2].

2. Оценка перспектив применения промышленного интернета вещей в России

В апреле 2021 г. Правительством России была обновлена методика оценки эффективности работы губернаторов, одним из главных показателей KPI которых стал показатель «цифровой зрелости» региона [7].

Цифровая зрелость – это индекс цифровизации региональных органов власти, местного самоуправления, а также организаций и учреждений в образовании, здравоохранении, строительстве и ЖКХ, общественном транспорте, использующих исключительно отечественные IT-решения, выраженный в процентах. В Постановлении Правительства РФ содержится информация о динамике роста

данного целевого показателя, в частности, к 2030 г. цифровая зрелость всех российских регионов должна составлять 100 % (построено авторами по [18]).

По существующей методике Правительства РФ возможно определить следующие уровни цифровой зрелости региона, представленные в табл. 1.

Таблица 1

Уровни «цифровой зрелости региона» России

№ п/п	Диапазон индекса «цифровой зрелости», %	Уровень цифровой зрелости региона
1	96–100	Очень высокий
2	76–95	Высокий
3	50–75	Достаточный
4	26–49	Низкий
5	11-25	Очень низкий
6	0–10	Критически низкий

Примечание: разработана авторами по: [6].

На рис. 1 представлена визуализация модели IIoT-зрелости принимаемых решений российскими компаниями.

Рис. 1. Моделирование IIoT-зрелости принимаемых решений

Примечание: разработано авторами по материалам Компании «Центр 2М» [17].

этап 1 – определение совокупности применяемых устройств, объединение их на IIoT-платформе и создание Единого центра управления и мониторинга;

этап 2 – обеспечение эффективной и бесперебойной связи между устройствами посредством Федерального мобильного оператора. Ожидается, что к концу 2025 года свыше 25% IIoT-устройств будет подключены через eSIM [16];

этап 3 – применение IIoT платформы и типа связи M2M (Machine-to-Machine, взаимодействие «от машины к машине»); осуществление управляемого подключения совокупности устройств с функцией биллинга данных;

этап 4 – функционирование платформы хранения и аналитики данных в целях обеспечения аутентичности IIoT-устройств и киберзащиты информации от хакерских атак и утечки данных;

этап 5 – работа IIoT-приложений и сервисов, доработка конкретных приложений под требования и специфику российских компаний, создание экосистем;

этап 6 – обеспечение кибербезопасности работы российской компании с использованием надежных информационно-технологических решений;

этап 7 – технологическая поддержка информационно-технологических решений по принципу «от устройства до платформы»;

этап 8 – осуществление процесса интеграции технологических возможностей IIoT-интеграторов в конкретных сферах деятельности (транспорте, энергетике, логистике и т. п.);

этап 9 – оценка эффективности IIoT-решений с применением различных подходов (инвестиционного анализа, построения экономико-математических и имитационных моделей, оценки экономического эффекта и пр.).

На рис. 2 представлена статистика проникновения рынка промышленного интернета по отраслям в Российской Федерации, выраженная в процентах.

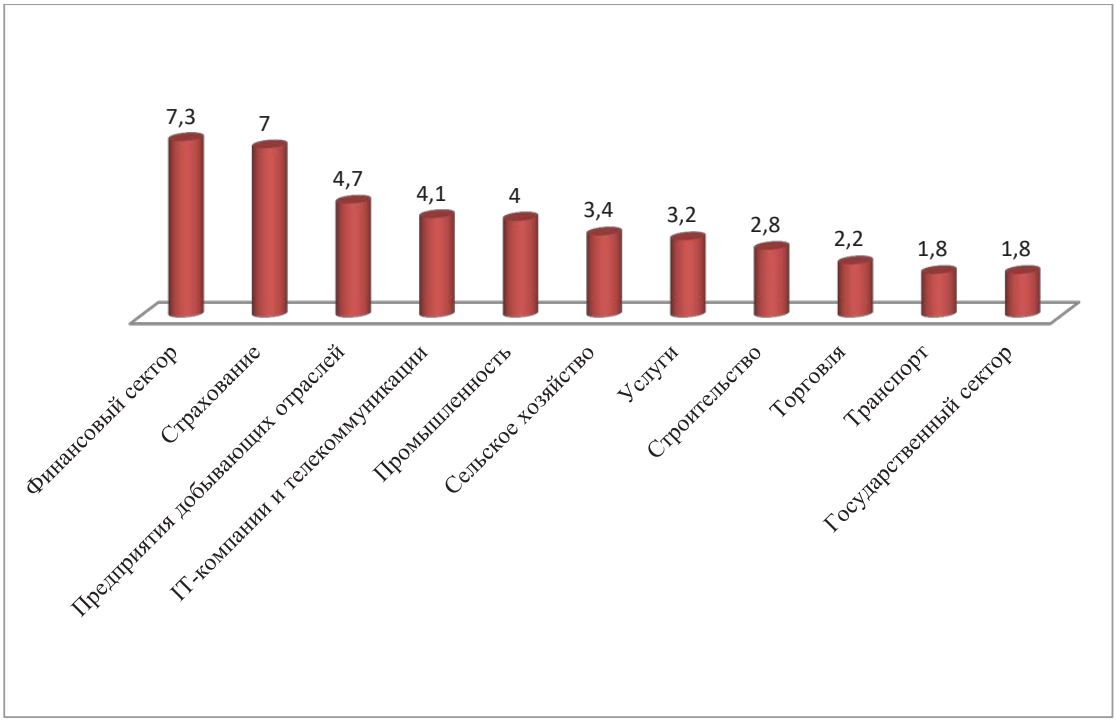

Рис. 2. Степень проникновения промышленного интернета в сферы российской экономики, в процентах

Примечание: построено авторами по материалам компании Центр 2М по состоянию на 2019 г. [12].

3. Анализ технологических и экономических характеристик промышленного интернета вещей, имеющих частноправовое значение

Система промышленного интернета вещей включает в себя следующие подсистемы:

– уровень устройства, который относится к физическим компонентам, оборудованию (CPS, датчики, машины), – на этом уровне собираются данные;

– уровень обслуживания, состоящий из программных приложений для анализа данных;

– сетевой уровень, включающий сети связи, которые транспортируют данные на уровень обслуживания, а с уровня обслуживания – на следующий уровень;

– уровень контента, включающий устройства пользовательского интерфейса [20].

Подобная структура используется для характеристики архитектуры интернета вещей, которая, согласно одному из источников, включает следующие технологические уровни:

– конечные устройства – это объекты, которые образуют «вещи» (things) в интернете вещей;

– программное обеспечение;

– уровень коммуникации;

– платформа – это место, где все эти данные собираются, анализируются и передаются пользователю в удобной форме [29].

Для описания технологии интернета вещей используется аббревиатура ABCDE, по первым буквам следующих слов: Analytics (аналитика), BigData (большие данные), Connection (соединение, связь), Devices (устройства), Experience (уже имеющийся опыт решения проблем) [30].

В рекомендациях Международного союза электросвязи приводится эталонная модель IoT, которая включает в себя четыре уровня: устройства, поддержки услуг и поддержки приложений, сети, приложения, а также возможности управления и обеспечения безопасности, которые связаны с указанными уровнями [23].

Для выявления круга частноправовых вопросов, связанных с функционированием промышленного интернета вещей, обратимся к характеристикам экосистемы интернета вещей и бизнес-моделей, используемых при коммерческом внедрении интернета вещей, данных Международным союзом электросвязи.

Так, экосистема IoT состоит из участников, каждый из которых играет одну или более из следующих деловых ролей:

– поставщик платформы;

– поставщик приложений;

– поставщик устройств;

– абонент приложений;

– поставщик сети.

При этом в разных вариантах коммерческого внедрения интернета вещей между участниками могут существовать различные взаимосвязи. Основными бизнес-моделями являются следующие:

1) модель, в которой один участник эксплуатирует устройство, сеть, платформу и приложения и напрямую обслуживает абонента приложений;

2) модель, в которой один участник эксплуатирует устройство, сеть и платформу, а другой – эксплуатирует приложение и обслуживает абонентов приложений;

3) модель, в которой один участник эксплуатирует сеть и платформу, другой – устройство и приложения и обслуживает абонентов приложений;

4) модель, в которой один участник эксплуатирует только сеть, другой – устройство и платформу, предоставляя приложения абонентам приложений;

5) модель, в которой один участник эксплуатирует только сеть, другой – платформу, а третий – устройства и предоставляет приложения абонентам приложений [23].

4. Выявление круга частноправовых вопросов промышленного интернета вещей на основе его технологических и экономических характеристик

Далее выявим характеристики промышленного интернета вещей, которые имеют частноправовое значение, основываясь на его технологических и экономических особенностях. Сосредоточимся вначале на выделении объектов, по поводу которых могут возникать частные правоотношения.

Так, уровень устройств связан с физическими объектами, вещами, которые являются объектами гражданских прав. При этом под устройствами (вещами, things) в аспекте интернета вещей понимаются не физические вещи, к которым подключены датчики, считывающие информацию о функционировании этих вещей, а сами датчики, которые являются более сложными устройствами, чем просто вещи: они, как правило, представляют собой физический объект с программным обеспечением.

Уровень устройств, а также уровень программного обеспечения (в других терминах – уровень обслуживания) и уровень приложений (в других терминах – уровень контента) связаны с использованием нематериальных объектов – технологий, компьютерных программ, баз данных и тому подобных результатов интеллектуальной деятельности, которые также являются объектами гражданских прав.

Сетевой уровень (в других терминах – уровень коммуникации, соединения, связи, сети) связан с оказанием услуг связи, как правило, акторами, внешними для обладателя такой системы управления, как промышленный интернет вещей.

Уровни устройств и программного обеспечения также могут быть связаны с выполнением работ или оказанием услуг внешними субъектами – работами по установке специального оборудования, услугами по хранению информации и др. Результаты работ и оказание услуг являются объектами гражданских прав.

Кроме того, использование технологий промышленного интернета вещей не исключает полностью человеческого участия в производственных процессах на разных уровнях, следовательно, применяется труд работников, выступающих объектом трудовых правоотношений, который зачастую характеризуется дистанционной составляющей – удаленным участием в управлении производственными процессами.

Итак, мы выделили объекты частных прав, по поводу которых могут возникать правоотношения, являющиеся предметом регулирования частного права: отношения, вытекающие из договоров о передаче интеллектуальных прав (об их отчуждении или лицензионных договоров), договоров об оказании услуг (услуг связи и иных), выполнении работ, трудовых договоров.

Все сказанное выше перекликается с выводами, сделанными авторами настоящего исследования ранее по поводу правового понимания интернета вещей. Авторами было предложено несколько подходов к такому пониманию: техноло-

гический (IoT как совокупность информационно-коммуникационных технологий), вещно-объектный (рассмотрение IoT с точки зрения вещей, потребительские свойства которых меняются с помощью применения этой технологии), системный (IoT как система правоотношений) [32].

Как видим, выделение технологических характеристик промышленного интернета вещей, имеющих частноправовое значение, в сравнении с приведенными выше подходами к его правовому пониманию показывает, что из технологических характеристик выпадает описание интернета вещей с точки зрения тех вещей, на потребительские свойства которых влияет технология IoT. Однако вещно-объектный подход в промышленном интернете вещей существует для характеристики уровня устройств, которые представляют собой физические объекты (датчики, сенсоры и т. п.). В потребительском интернете вещей этот уровень смещается в сторону усиления, изменения потребительских качеств товара, а в промышленном интернете вещей – в сторону усиления, изменения возможностей по управлению производством.

Публикация Международного союза электросвязи показывает многообразие правоотношений между участниками интернета вещей. Это влияет на систему договоров, заключаемых по поводу функционирования промышленного интернета вещей и их содержание. Во многих случаях это могут быть смешанные договоры, т. к. субъекты могут брать на себя несколько деловых ролей. Однако можно выявить систему договоров, которые обслуживают функционирование промышленного интернета вещей, по критерию их роли, выполняемой в функционировании промышленного интернета вещей:

1) договоры, которые направлены на обеспечение функционирования устройств. Это может быть, например, договор поставки устройств, договор подряда, договор оказания услуг по техническому обслуживанию. В связи с тем, что элементами устройств может быть программное обеспечение, это могут быть в дополнение к перечисленным, договоры о передаче интеллектуальных прав;

2) договоры, направленные на обеспечение функционирования программных продуктов. Это договоры о передаче исключительных прав, как правило, лицензионные договоры с исключительной или неисключительной лицензией;

3) договоры, направленные на обеспечение функционирования приложений, которые используются для аналитики данных и воспроизведения их результатов. Это могут быть договоры о передаче интеллектуальных прав по использованию приложений, договоры оказания информационных услуг: услуг по обработке информации (данных), по предоставлению информации, по хранению информации. Информация, выступающая объектом воздействия услуг в таких договорах, является результатом сбора данных устройствами и анализа этих данных;

4) договоры, направленные на обеспечение связи между всеми элементами промышленного интернета вещей. Это договоры об оказании услуг связи, например, беспроводной связи, услуг доступа к интернету и др.

В том случае, если полное функционирование промышленного интернета вещей обеспечивается одним субъектом по заказу другого, может заключаться договор об оказании услуг по управлению предприятием, где управление имеет

не корпоративный, а технологический характер – управление производственными процессами.

Заключение. Настоящее исследование позволило сделать следующие выводы.

1. Развитие промышленного интернета вещей в РФ позволит осуществить инновационную цифровую трансформацию производственного сектора и бизнес-процессов, получить при этом существенную экономию денежных средств и сокращение сроков окупаемости капитальных вложений на процесс реализации принятых решений, исключить из большей части технологических процессов и операций участие субъекта.

2. Авторами смоделирована IIoT-зрелость российских компаний, развит алгоритм принятия IIoT-решений российских компаний, учтен фактор цифровой трансформации в принятой Правительством России методике оценки цифровой зрелости.

3. Частноправовое значение имеет технологическая структура промышленного интернета вещей, а именно деление его на технологические уровни, в которые входят уровни устройств, программного обеспечения, пользовательских приложений, связи.

4. Технологическое устройство промышленного интернета вещей позволяет выделить в нем существование объектов гражданских прав, среди которых физические вещи, результаты интеллектуальной деятельности, оказание услуг, результаты работ, а также более сложные объекты, представляющие собой сочетание физической вещи с программным обеспечением. Такой симбиоз придает объекту особые свойства. Как уже отмечалось в предыдущих исследованиях, необходимо продумать введение в гражданское право таких особых, симбиозных, объектов: «вещь + программа для ЭВМ», «вещь + программа для ЭВМ+услуга» [32, 33].

5. Бизнес-модели, используемые при коммерческом внедрении промышленного интернета вещей, свидетельствуют о многообразии договорных связей, существующих для обеспечения функционирования промышленного интернета вещей.

6. Авторами предложено построение системы договоров, которые обслуживают функционирование промышленного интернета вещей, по критерию их роли, выполняемой в обеспечении этого функционирования:

1) договоры, которые направлены на обеспечение функционирования устройств;

2) договоры, направленные на обеспечение функционирования программных продуктов;

3) договоры, направленные на обеспечение функционирования приложений;

4) договоры, направленные на обеспечение связи между всеми элементами промышленного интернета вещей.

Все эти договоры могут стать элементами единого договора об оказании услуг по управлению производственными процессами.

7. Система договоров может строиться и по другим критериям, например видам субъектов, заключающих договоры, в зависимости от их деловой роли.

8. Подтверждены выдвинутые авторами научные гипотезы о том, что технологические и экономические характеристики промышленного интернета вещей имеют частноправовое значение, правовой режим промышленного интернета вещей включает не только правила частноправового характера, предложенные авторами ранее подходы к правовому пониманию интернета вещей вытекают из его технологических и экономических характеристик.

Список литературы

1. Александров С. В., Макаревич М. Л. Интернет вещей. Вопросы правового регулирования // Современные подходы к трансформации концепций государственного регулирования и управления в социально-экономических системах: сборник научных трудов 7-й Международной научно-практической конференции, Курск, 20–21 февраля 2018 г. Курск: Университетская книга, 2018. С. 11-16.

2. Ануфриенко А. Ю. Применение средств «Интернета вещей» для автоматизации управления жизненным циклом // Вопросы инновационной экономики. 2020. Т. 10, № 3. С. 1093-1100.

3. Бартко И. А. Правовая охрана цифровых вещей в сети интернет // Via Scientiarum – Дорога знаний. 2021. № 4. С. 18-22.

4. Бундин М. В. Новые тенденции в правовом регулировании персональных данных и будут ли они по-прежнему принадлежать личности // Законность и правопорядок. 2018. № 3(19). С. 4-8.

5. Галицкая Н. В. Право на кибербезопасность: опыт Евросоюза // Права человека и политика права в XXI в.: перспективы и вызовы: сборник научных трудов по итогам Всероссийской научно-практической конференции с международным участием, Москва, 27-28 мая 2022 г. Саратов: Саратовский источник, 2022. С. 440-449.

6. Городнова Н. В. Метод оценки качества информационных потоков при формировании big data в цифровой экономике // Вопросы инновационной экономики. 2022. Т. 12, № 1. С. 607-624.

7. Губернаторов оценят по «цифровой зрелости» регионов. URL: https://www.cnews.ru

8. Гуляев К. С. Право человека на Интернет, права в Интернете и при использовании Интернет-вещей: новые тенденции // Прецеденты Европейского суда по правам человека. 2018. № 1(49). С. 29-38.

9. Жернова В. М. Предпосылки развития информационного законодательства на примере киберфизических систем // Вестник УрФО. Безопасность в информационной сфере. 2021. № 2(40). С. 59-64.

10. Забайкин Ю. В., Лунькин Д. А. Направления развития права в сфере Интернета вещей // Вопросы российского и международного права. 2023. Т. 13, № 1-2-1. С. 208-214.

11. Зинковский М. А. «Технологии управляемого старения» товаров в договорах с потребителями // Хозяйство и право. 2022. № 8(547). С. 12-20.

12. Интернет вещей, IoT, M2M, рынок России. URL: https://www.tadviser.ru

13. Иншакова А. О. Право как основа инфраструктурного обеспечения цифровой экономики и технологии Интернета вещей // Правовая парадигма. 2019. Т. 18, № 3. С. 6-11.

14. Купцова А. С. Правовое регулирование использования интернета вещей // Образование и право. 2021. № 7. С. 225-230.

15. Мефодьева К. А. Цифровые данные в предпринимательском обороте на примере применения Интернета вещей в аграрной сфере: правовые аспекты // Аграрное и земельное право. 2018. № 8(164). С. 143-148.

16. Овсянников М. В., Подкопаев С. А. Облачная система управления производством в рамках жизненного цикла продукции на основе интернета вещей // Вопросы инновационной экономики. 2020. Т. 10, № 3. С. 1311-1318.

17. Официальный сайт компании «Центр 2М». URL: https://center2m.ru

18. Постановление Правительства РФ от 3 апреля 2021 г. № 542 «Об утверждении методик расчета показателей для оценки эффективности деятельности высших должностных лиц (руководителей высших исполнительных органов государственной власти) субъектов Российской Федерации и деятельности органов исполнительной власти субъектов Российской Федерации, а также о признании утратившими силу отдельных положений Постановления Правительства Российской Федерации от 17 июля 2019 г. № 915». URL: http://ivo.garant.ru

19. Правовое регулирование отношений по оказанию услуг в условиях цифровой экономики: доктринальные, нормотворческие и правоприменительные аспекты: монография / М. А. Бажина, Н. В. Городнова, О. В. Жевняк [и др.]; под общ. ред. д-ра юрид. наук, проф. Е. Г. Шабловой; М-во науки и высш. образования РФ. Екатеринбург: Изд-во Урал. ун-та, 2023. 300 с.

20. Промышленный интернет вещей. URL: https://ru.wikipedia.org

21. Промышленный интернет вещей: определение, принцип работы, настоящее и перспективы. URL: https://future2day.ru

22. Пушкарев М. С. Интернет вещей (IoT): понятие и значение для формирования правовой основы цифровой трансформации экономики // Вопросы российского и международного права. 2018. Т. 8, № 1А. С. 16-27.

23. Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений – Структура и функциональные модели архитектуры. Обзор Интернета вещей. URL: http://handle.itu.int/11.1002/1000/11559

24. Савельев А. И. Направления эволюции свободы договора под влиянием современных информационных технологий // Свобода договора: сборник статей / Московский государственный юридический университет имени О. Е. Кутафина. Москва: СТАТУТ, 2016. С. 481-542.

25. Сараева А. А. Применение технологии «Промышленный интернет вещей» на предприятии // Политехнический молодежный журнал. 2021. № 11(64).

26. Сумикова И. П. Промышленный интернет вещей: перспективы и риски использования в производстве // Актуальные научные исследования в современном мире. 2021. № 11-8(78). С. 155-159.

27. Тягай Е. Д. Интернет вещей и охрана интеллектуальной собственности в бизнесе: новые вызовы времени // Журнал Суда по интеллектуальным правам. 2017. № 15. С. 57-64.

28. Филипова И. А. Цифровое будущее: сфера труда и управление ее трансформацией с помощью права // Трудовое и социальное право. 2021. № 3(39). С. 30-34.

29. Что такое IoT и что о нем следует знать. URL: https://habr.com/ru/companies/otus/articles/549550/

30. Что такое интернет вещей и как он устроен. URL: https://trends.rbc.ru/trends/industry/5db96f769a7947561444f118

31. Шаблова Е. Г., Городнова Н. В., Жевняк О. В. Региональное регулирование промышленного Интернета вещей на примере Свердловской области // Креативная экономика. 2022. Т. 16, № 9. С. 3435-3454.

32. Шаблова Е. Г., Жевняк О. В. Разработка концепции правового режима промышленного интернета вещей // Право и экономика. 2022. № 10(416). С. 24-32.

33. Шаблова Е. Г. Проблемы гражданско-правового регулирования отношений об оказании услуг в свете тенденций цифровизации экономики // Вестник экономики, права и социологии. 2019. № 4. С. 147-151.

34. Шеве Г., Хюзиг С., Гумерова Г. И., Шаймиева Э. Ш. Индустрия 4.0 (Германия). Промышленный интернет вещей (Industrial Internet of Things) (США): разграничение понятий // Инвестиции в России. 2019. № 11(298). С. 3-8.

35. Boyes H., Isbell R. and Watson T. Critical infrastructure in the future city -developing secure and resilient cyber-physical systems. In: 9th International Conference on Critical Information Infrastructures Security, Limassol, Cyprus, 13-15 Oct 2014. URL: https://www.researchgate.net

36. Industrial Internet of Things – IioT. Промышленный интернет вещей. URL: https://www.tadviser.ru

37. Industrial Internet of Things – IioT. Промышленный интернет вещей в России. URL: https://www.tadviser.ru

38. Schwab K. The fourth industrial revolution. First U.S. edition. New York: Crown Business, 2017.

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ТРУДОВЫХ И СВЯЗАННЫХ С НИМИ ПРАВООТНОШЕНИЙ

DIGITAL TECHNOLOGIES IN THE SYSTEM OF LABOR AND ADJACENT RELATIONS

А. С. Кашлакова,
кандидат юридических наук, доцент,
Всероссийский государственный университет юстиции
(РПА Минюста России),
Сочинский филиал

НЕКОТОРЫЕ ПРОБЛЕМЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ТРУДА В МЕТАВСЕЛЕННОЙ

Аннотация. Целью настоящей статьи является исследование особенностей реализации труда в метавселенных. На основе изучения современного состояния развития метавселенных выявлены особенности отношений, реализуемых с помощью данной технологии, что обусловливает необходимость специального подхода в правовом регулировании этих отношений. Установлено, что нормы действующего законодательства, принятые для регулирования отношений в физическом мире, не учитывают специфики отношений в виртуальной реальности и не способны обеспечить их адекватное правовое регулирование. В работе предпринята попытка дифференцированного подхода к изучению трудовых отношений в метавселенных в зависимости от степени использования этой технологии от применения метавселенных в качестве дополнительной возможности к традиционным трудовым отношениям к трудовым отношениям, протекающим только в метавселенной и до применения метавселенной наряду с осуществлением трудовой функции также и для досуга и развлечений. В зависимости от варианта использования метавселенной меняется и необходимость в регулировании отдельных аспектов правоотношений и защиты определенных прав. В этой связи обозначены некоторые проблемы правового регулирования трудовых отношений и предложены варианты их решения.

Ключевые слова: право, цифровые технологии, метавселенная, труд, трудовые отношения, конфиденциальность, применимое право

SOME PROBLEMS OF THE LEGAL REGULATION OF LABOR IN THE METUNIVERSE

Abstract. The purpose of this article is to study the features of the implementation of labor in metauniverses. Based on the study of the current state of the development of metauniverses, the features of relations implemented using this technology are revealed, which necessitates a special approach in the legal regulation of these relations. It has

been established that the norms of the current legislation adopted to regulate relations in the physical world do not take into account the specifics of relations in virtual reality and are not able to provide their adequate legal regulation. The paper attempts to make a differentiated approach to the study of labor relations in the metauniverses, depending on the degree of use of this technology, from the use of metaverses as an additional opportunity to traditional labor relations to labor relations that occur only in the metaverse and before the use of the metauniverse, along with the implementation of the labor function also for leisure and entertainment. Depending on the use of the metaverse, the need to regulate certain aspects of legal relations and protect certain rights also changes. In this regard, some problems of legal regulation of labor relations are identified and options for their solution are proposed.

Keywords: law, digital technologies, metaverse, labour, labor relations, confidentiality, applicable law

В условиях быстро развивающихся цифровых технологий и цифровой экономики развитие получают метавселенные. Правовые аспекты регулирования метавселенных обсуждают в Совете Федерации, о необходимости использовать возможности метавселенных, чтобы люди могли общаться, работать, учиться, реализовывать совместные творческие и деловые проекты, невзирая на расстояния, заявил Президент России [4]. На этом фоне можно наблюдать отставание правового регулирования отношений, в том числе и трудовых, в условиях новой реальности.

Еще не решен ряд вопросов, возникших в связи с развитием цифровизации, повлекшей распространение нетипичных форм занятости, адаптации деловых качеств работника к внедрению новых технологий, роботов, искусственного интеллекта, увеличение риска доступа к личной информации работника, нарушение права на конфиденциальность и автономию личности при применении новых технологий, мониторинга трудовой деятельности работника и других рисков реализации прав человека в сфере труда, пришли более прогрессивные технологии, усиливающие непонимание и риски в области права, в том числе и трудового. Так, в частности, к перечисленным нерешенным вопросам добавляется и проблема реализации права на труд в условиях метавселенных, набирающих обороты в последнее время по всему миру.

Представители разных компаний делают свои ставки в развитии метавселенных, в том числе игры, социальные сети, синтез кино, игр, медиа и т. п. Поскольку метавселенная интегрирует виртуальную, дополненную и физическую реальность, в которой люди с использованием аватаров вступают друг с другом в отношения, необходимо разрабатывать нормы, устанавливающие правила такого взаимодействия, тем более что концепция метавселенной вышла за пределы компьютерных игр и развлечений и распространяется уже не только на цифровую среду промышленности и бизнеса. В метавселенных теперь проводят свадебные церемонии [9], защит дипломов [16, 18] и диссертаций [8] и т. п. Среди возможностей, которые предоставляет метавселенная, есть, помимо прочих, подробно описанных в литературе, также и организация труда, служебных отношений, политических ин-

ститутов [11. С. 3]. Кроме этого, метавселенные используют и для осуществления государственной власти, в том числе и судебной. Так, известно о рассмотрении судебного дела в метавселенной. 15 февраля 2023 года Административный суд департамента Магдалена в Колумбии впервые провел заседание в метавселенной по делу, инициированному региональным транспортным профсоюзом против полиции, и собирается продолжать эксперименты с виртуальной реальностью [10]. Ранее судья в Колумбии использовал нейросеть ChatGPT для консультации перед вынесением приговора. Дело касалось покрытия расходов на медицину и транспорт для ребенка с расстройством аутистического спектра. В итоге решение суда совпало с ответом чат-бота [17].

В прессе широко также обсуждали открытие Барбадосом своего посольства в метавселенной [3], которое оказалось не первым [14]. 16 января 2023 года власти столицы Южной Кореи открыли для пользователей проект Metaverse Seoul. По данным Forkast, крупные южнокорейские компании Samsung Electronics, SK Telecom и Naver уже организовали свои виртуальные представительства в Metaverse Seoul [24]. Понятно, что деятельность всех этих цифровых посольств должны обеспечить реальные люди, которые вовлекаются в программу с помощью технических устройств.

Все эти примеры свидетельствуют о том, что метавселенные уже вошли в нашу жизнь и не только с точки зрения развлечений и досуга, но и распространяются на учебные, рабочие процессы, взаимодействие с властью. Все это вызывает вопрос о правовом регулировании отношений в метавселенных, которое на сегодняшний день отсутствует. Может возникнуть идея о том, что, поскольку виртуальная реальность является отражением физической реальности и коммуницируют в ней реальные лица, но через аватары, то к отношениям в виртуальной реальности вполне применимы имеющиеся нормы законодательства. Однако действующее законодательство не учитывает особенностей виртуальной реальности, в том числе и специфики коммуникации субъектов в ней, которая, безусловно, имеется. Как минимум это проявляется в субъекте правоотношений, действующем через аватар (альтерэго), а также в объекте, который возможно создать и вывести из метавселенной в физический мир (например, токены), но не наоборот.

В настоящее время ряд стран обеспокоены правовым регулированием отношений в метавселенных [19. С. 58]. Его отсутствие на сегодняшний день оборачивается инцидентами, не защищенными со стороны права. Так, например, в декабре 2022 года 43-летняя докторант-исследователь Нина Джейн Патель подверглась тому, что она назвала сексуальным насилием в метавселенной. Примечательно, что Патель является докторантом-исследователем в Университете Рединга, изучающим «психологическое и физиологическое воздействие» погружения в виртуальные миры, и знает, как может ощущаться нарушение цифрового взаимодействия [25]. Есть и другие примеры некорректного поведения в метавселенных, вызывающих определенное беспокойство [7. С. 49].

С точки зрения проводимого исследования нас больше интересует осуществление трудовых, служебных обязанностей в метавселенных, хотя, конечно же, общее развитие метавселенных для разных целей не может не сказываться на сте-

пени защищенности прав работников в метавселенных. Так, Стив Найджел, глава Microsoft, говорит о «виртуальных рабочих коммуникациях», имея в виду виртуальный офис или «фабрику» [23]. Как это происходит с точки зрения осуществления трудовой функции, в одной из своих работ описал М. Биаси, принявший участие в одном из совещаний в метавселенной весной 2022 года, когда его друг пригласил присоединиться к одной из виртуальных встреч, которые он еженедельно проводил в метавселенной со своими помощниками, физически находившимися в различных частях мира. Пребывание в пространстве происходило при помощи гарнитуры и пары контроллеров (похожих на те, что используются в видеоиграх), имевшее очень мало общего с такими платформами, как Microsoft Teams и Google Meet, где со времен пандемии очень много рабочих встреч проводится удаленно. В виртуальном, иммерсивном измерении участники могли взаимодействовать через свои виртуальные альтерэго (аватары), что больше напоминало живую, чем онлайн-встречу. В трехмерном пространстве можно было проецировать изображения и графику на стены, обмениваться документами и файлами и в более общем плане перемещаться по конференц-залу. Самое главное, два из пяти чувств (зрение и слух) были задействованы с такой степенью реализма, которая не имела аналогов ни в одной из предыдущих двумерных виртуальных встреч [22].

Перспектива применения метавселенных в трудо-правовой сфере в России достаточно велика, что подтверждается совместным исследованием консалтингового агентства Jobby и компании Kometa и RB.RU. Его результаты были представлены на виртуальном бранче в метавселенной Pixity [13].

Таким образом, выполнение рабочих функций в метавселенной – это уже не перспектива будущего, а реальность, которая используется не только для досуга и развлечений, но и для ведения предпринимательской деятельности, осуществления государственной власти. Сегодня бессмысленно отрицать тот факт, что метавселенные вошли в нашу жизнь, и дальше их распространение будет набирать обороты. Они являются удобной платформой для самых разнообразных целей, обладающих рядом преимуществ перед другими, более традиционными формами существования общественных отношений. Сокращаются расходы на эксплуатацию рабочих мест, доступ к рабочему месту возможен из любой точки мира, что является привлекательным не только для работника, но и работодателя, особенно в крупных организациях, имеющих филиалы не только в разных городах, но и странах.

Исходя из имеющихся примеров метавселенной, можно выделить три возможных варианта реализации трудовых отношений в метавселенной.

Первый вариант предполагает использование метавселенной как дополнительной технологии для выполнения отдельных трудовых обязанностей по участию, например, в рабочих совещаниях. В настоящее время такими технологиями в основном являются Zoom, MicrasoftTeams и другие программы для онлайн-встреч. В данном случае работник четко осознает цель входа в метавселенную, его пребывание в данном пространстве ограничено временем и поставленными задачами, поэтому возможности осуществления мониторинга за его поведением со стороны работодателя ограничены, в том числе и из-за способности работника более

четко концентрироваться на определенное время на поставленных задачах и не допускать посторонних эмоций, которые могут подвергаться мониторингу и анализу со стороны работодателя. Конечно, уже здесь имеются риски нарушения прав человека на личную информацию, такую, например, как контроль самочувствия работника, его вовлеченность в процесс, заинтересованность встречей, реакция на обсуждаемые вопросы и полученную от собеседников информацию и т. п. [20], что становится возможным вследствие использования определенного оборудования (специальные шлемы, очки, другая гарнитура) и отсутствия государственного регулирования рассматриваемых вопросов.

Второй вариант предполагает использование метавселенной как единственного места выполнения трудовых обязанностей. В данном случае, учитывая более длительное время пребывания на платформе, возможности осуществлять мониторинг за поведением и качествами работника, не относящимися к деловым, потенциально увеличены.

Третий вариант использования метавселенной напоминает «вторую жизнь» и предполагает использование ее не только как места выполнения трудовых обязанностей, но также и места проведения досуга, участия в играх, посещения выставок, концертов, занятия шопингом, возможно, личных встреч, занятия предпринимательской деятельностью и т. п. Излишне говорить, что работодателю при таком варианте использования метавселенной доступна практически вся информация о работнике, о его качествах, как связанных, так и не связанных с выполнением трудовых обязанностей.

С точки зрения правового регулирования можно констатировать, что регулирование труда в метовселенных усложняется от первого варианта, наиболее понятного и простого, к третьему, наиболее сложному, вызывающему много вопросов как с точки зрения применения уже имеющихся норм, так и выявления полного отсутствия норм, способных урегулировать разные аспекты таких отношений.

Как уже было сказано, наиболее понятным и простым будет регулирование первого варианта работы в метавселенной, при котором она используется как дополнительная технология. Пожалуй, единственное, о чем можно беспокоиться работнику при осуществлении труда с применением такой новой технологии – это о степени осуществления контроля со стороны работодателя, потенциально способного выйти за пределы необходимого и разумного. Конфиденциальность с развитием новых технологий является наиболее уязвимой темой и приобретает в данном случае новые аспекты. Если до сих пор проблемными вопросами являлись хранение, обработка, передача, уничтожение информации о работнике, а также использование сведений о работнике из свободного доступа, то при использовании технологии метавселенной многие вопросы для работодателя решаются сами собой, так как отслеживание личной информации становится возможным непосредственно на платформе в период активности работника. Более того, применение метавселенных обнаруживает возможность незаконного доступа к таким личным данным работника, которые ранее работодателю просто неоткуда было получить, особенно при втором и третьем вариантах работы в метавселенной. Например, при выборе определенной роли в игре за поведением игрока и за при-

нятием им решений можно наблюдать непосредственно в игре и на этой основе принимать решения в реальной жизни [2]. То есть поведение человека в виртуальной реальности может повлиять на принятие определенных решений в реальной жизни, что может быть негативным с точки зрения реализации отдельных прав. Налицо такая проблема, как стирание права на конфиденциальность и автономию, грани между личной жизнью и публичностью. Если сейчас этот вопрос решается как минимум самим субъектом, который может внимательно относиться к следам в Интернете и предпринимать усилия для сохранения тайны о личной жизни, то в метавселенных конфиденциальность практически невозможна.

Таким образом, по мере погружения («ухода») работника в метавселенную у работодателя расширяется возможность осуществлять мониторинг не только за «трудовой жизнью» работника, но и за его «виртуальной жизнью» вообще. Работодатель может, помимо прочего, анализировать поведение работника и в нерабочее время, не утруждаясь поиском необходимой информации в Интернете, социальных сетях. Для работодателя становится доступной информация об увлечениях, предпочтениях, склонностях, хобби и т. п. Такой доступ работодателя к личной информации работника увеличивает риск нарушения прав работников принятием решений работодателем на основе такой личной информации. Можно констатировать, что в пределах метавселенной частной жизни у такого работника практически нет, что делает его предельно уязвимым.

Кроме конфиденциальности также обнаруживает себя проблема применимого права. Как уже было сказано, метавселенная является удобной технологией, ее используют, в том числе при необходимости преодоления пространственных расстояний, когда работники находятся не только в разных городах одной страны, но и в разных частях мира. Возникает вопрос о применимом праве. В соответствии с частью пятой ст. 11 ТК РФ [1], на территории Российской Федерации правила, установленные трудовым законодательством и иными актами, содержащими нормы трудового права, распространяются на трудовые отношения с участием иностранных граждан, лиц без гражданства, организаций, созданных или учрежденных иностранными гражданами, лицами без гражданства либо с их участием, международных организаций и иностранных юридических лиц, если иное не предусмотрено ТК РФ, другими федеральными законами или международным договором Российской Федерации. То есть применяется законодательство места выполнения работы (lex loci laboris).

Однако применение таких технологий, как метавселенная, вызывает вопрос о территориальности выполнения труда как со стороны работодателя, так и со стороны работника. Стоит ли придерживаться правил, сформулированных для регулирования отношений, возникающих на определенной территории, если отношения возникают и осуществляются не на территории, а в виртуальном пространстве? Стоит признать, что действующие нормы трудового законодательства, регулирующие отношения с иностранным элементом, не учитывают возникающих новых форм трудовых отношений настолько, что создают определенную проблему.

Так, в случае если работодателем является российская организация, использующая технологию метавселенной, прием на работу работников, являющихся

иностранными лицами, должен осуществляться в соответствии с нормами главы 50.1. ТК РФ [1]. Однако нормы данной главы ориентированы на регулирование трудовых отношений с иностранными лицами, въезжающими и пребывающими (проживающими) на территории России, что связано непосредственно с миграционной политикой. Если же речь идет о «виртуальном присутствии», то многие положения не просто теряют смысл, но и создают препятствия для заключения трудовых договоров в метавселенной, как то: императивные требования о предоставлении разрешения на работу или патента, разрешении на временное проживание, разрешения на временное проживание в целях получения образования, вида на жительство (ст. 327.2 ТК РФ).

Нормы о дистанционной работе главы 49.1 ТК РФ также не могут быть применены для регулирования труда в метавселенной. Объединяющим дистанционную работы и работу в метавселенной является использование сети Интернет. Однако в целом эти формы труда имеют больше различий, чем общего. Смысл дистанционной работы заключается в том, что она выполняется дистанционно (удаленно) от работодателя. Дистанционный работник самостоятелен в определении рабочего места, а также в организации рабочего времени и времени отдыха, что исключает прямой или косвенный контроль со стороны работодателя за процессом выполнения работы. Чего нельзя сказать о работе в метавселенных, где работа происходит в пространстве, принадлежащем работодателю, кроме того, эта работа осуществляется под прямым контролем работодателя. Насколько «внимательным» будет такой контроль, решает работодатель. Главное – это то, что виртуальное рабочее место находится в постоянном доступе для осуществления контроля. Более того, сам контроль может быть более пристальным, выходящим за пределы разумного и необходимого, о чем уже было сказано ранее.

Стоит признать, что нормы, регулирующие трудовые отношения с иностранным элементом, не адаптированы под новые формы труда, имеют территориальную привязку, которая не только не важна при осуществлении труда в новых формах, но и является излишней. Это требует выработки новых подходов в формулировании коллизионных норм, направленных на регулирование труда с иностранным элементом.

В ст. 11 ТК РФ приоритетное применение получило правило lex loci laboris. В литературе оно обосновано рядом причин, в числе которых интеграция работника в трудовой коллектив, участие работника в разных формах социального партнерства, определенность в действии локальных нормативных актов, а также определенность в подсудности дела в случае возникновения трудового спора [6. С. 54, 55; 5]. Однако, как уже было сказано, в настоящее время возникают такие формы труда, при которых работник не интегрируется в коллектив, не участвует в социальном партнерстве, поэтому настаивать на приоритетном применении правила lex loci laboris становится неактуальным. Наиболее соответствующим современному состоянию отношений в сфере труда является применение правила lex voluntatis, о чем уже было сказано в научной литературе [12. С. 77], по этому пути пошли и некоторые страны [15. С. 155].

Как представляется, наиболее подробно и последовательно коллизионные привязки при определении применимого права изложены в Регламенте (ЕС) № 593/2008 о праве, подлежащем применению к договорным обязательствам («Рим I») [21], в ст. 8 которого закреплены следующие коллизионные правила. Первым правилом является автономия воли lex voluntatis. В случае отсутствия выбора применяется правило lex loci laboris, то есть действует право той страны, в которой работник выполняет трудовые обязанности. Если правило lex loci laboris невозможно применить вследствие неопределенности места выполнения работ, то применяется законодательство места нахождения работодателя, а в случае, если договор имеет явно более тесные связи с другой страной, чем та, в которой находится работник или работодатель, то применяется право этой другой страны. При применении коллизионной привязки о возможности выбора применимого законодательства действует правило о том, что этот выбор не может повлечь за собой лишение работника защиты, предоставляемой ему положениями, от которых не разрешается отступать посредством соглашения в соответствии с правом, которое при отсутствии выбора подлежало бы применению.

Изложенные коллизионные привязки в наибольшей степени соответствуют современному состоянию в сфере труда и могут быть использованы для интеграции их в российское законодательство.

Таким образом, подводя итог проведенному исследованию, приходим к следующим выводам. Метавселенная как новая технология набирает большие обороты для выполнения самых разных задач, в том числе и в сфере труда. Поскольку имеется специфика отношений, возникающих и реализуемых в метавселенной, а также возникают новые риски и угрозы, связанные с возможностями этой новой технологии по мониторингу за поведением работника как при выполнении трудовых обязанностей, так и при проведении досуга, требуется определенная реакция со стороны законодателя на эти новые возможности и риски. В связи с тем, что труд в метавселенной протекает не на территории, а в виртуальной реальности, необходимо пересмотреть нормы о применимом праве. Как представляется, наиболее современными являются правила выбора применимого права, изложенные в Регламенте «Рим I», которые могут быть учтены при изменении российского трудового законодательства.

Список литературы

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 3.

2. Агатеев В., Бузько Р. Юридические аспекты метавселенной. URL: https://www.buzko.legal/content-ru/yuridicheskie-aspekty-metavselennoy

3. Барбадос стал первым в мире государством с собственным посольством в метавселенной. URL: https://noi.md/ru/v-mire/barbados-stal-pervym-v-mire-gosudarstvom-s-sobstvennym-posolistvom-v-metavselennoj

4. В Совете Федерации обсудили правовые аспекты регулирования метавселенных. URL: http://council.gov.ru/events/main_themes/138419/

5. Дзарасов М. Э. Правовое регулирование труда работников-иностранцев // Lex russica. 2014. № 8. С. 940-946.

6. Довгерт А. С. Правовое регулирование международных трудовых отношений. Киев, 1992. 248 с.

7. Евсиков К. С. Метавселенные как новый объект регулирования для информационного права // Труды по интеллектуальной собственности (Works on Intellectual Property). 2023. Т. 44, № 1. С. 47-57.

8. Инновационный кофе Метавселенная: от теории к практике. URL: https://www.intesasanpaoloinnovationcenter.com/en/news-and-events/events/2023/03/innovation-coffee-metaverso-theory-practice/

9. Как прошла первая в России свадьба в метавселенной: модный диджей, NFT-подарки, донаты в крипте. URL: https://maff.io/media/russian_wedding_metaverse

10. Котов П. Колумбийский суд провел заседание в метавселенной. URL: https://3dnews.ru/1082538/kolumbiyskiy-sud-provyol-zasedanie-v-metavselennoy

11. Лескина Э. И. Метавселенная и задачи в области правового регулирования данных // Юрист. 2023. № 3. С. 2-7.

12. Лушникова М. В. Коллизионное правовое регулирование международных трудовых отношений: теоретические проблемы и современная практика // Закон. 2011. № 10. С. 68-77.

13. Печерская И. 70% российских HR-специалистов допускают, что метавселенные скоро заменят работу в офисе. URL: https://rb.ru/partners/research-jobby/

14. Получить визу Барбадоса можно будет в метавселенной. URL: https://www.vesti.ru/hitech/article/2640570

15. Правовое регулирование социально-трудовых отношений с иностранными гражданами: междисциплинарный подход: монография / под общ. ред. Е. Б. Хохлова, Е. В. Сыченко. М.: Юстицинформ, 2019. 320 с.

16. Студенты первой в России магистратуры по Fashion Tech отправятся защищать дипломы в метавселенную. URL: https://dzen.ru/a/ZHjMehMDahQmPN8R?utm_referer=yandex.ru

17. Суд Колумбии впервые провел совещание в метавселенной. URL: https://habr.com/ru/news/719010/

18. «Точка кипения – ПромТехДизайн» СПбГУПТД // Петербургские студенты впервые защитят дипломы в метавселенной. URL: https://spbdnevnik.ru/news/2023-06-02/peterburgskie-studenty-vpervye-zaschityat-diplomy-v-metavselennoy

19. Федоренко С. П. Метавселенная как фактор трансформации правового регулирования // Северо-Кавказский юридический вестник. 2023. № 1. С. 56-61.

20. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7-32. EDN LCCOJJ.

21. Regulation (EC) N 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) // OJ. L 177. 2008. Pp. 6-16.

22. Marco Biasi The Labour Side of the Metaverse // Italian Labour Law e-Journal. 2023. Vol. 16, Iss.1.

23. Meta-Worse – труд и права работника в новом прекрасном мире. URL: https://vc.ru/future/343787-meta-worse-trud-i-prava-rabotnika-v-novom-prekrasnom-mire
24. Metaverse Seoul – правительство Южной Кореи запустило долгожданную метавселенную с «госуслугами» и офисами брендов. URL: https://rb.ru/longread/metaverse-seoul/
25. Metaverse vs employment law: the reality of the virtual workplace. URL: https://www.ft.com/content/9463ed05-c847-425d-9051-482bd3a1e4b1

С. В. Коблов,
соискатель,
Научно-исследовательский институт образования и науки

РАЗВИТИЕ ЦИФРОВЫХ КОМПЕТЕНЦИЙ СОТРУДНИКОВ В ОРГАНИЗАЦИЯХ, ПРЕТЕРПЕВАЮЩИХ ЦИФРОВУЮ ТРАНСФОРМАЦИЮ

Аннотация. В статье рассматриваются цифровые компетенции, необходимые для успешной работы в современном мире. Описаны основные аспекты цифровых компетенций: эффективность, инновационность, гибкость, ответственность и саморазвитие. Рассматриваются проблемы при формировании цифровых компетенций в организации. Приводится перечень организационных мероприятий, которые способствуют приращению цифрового капитала компании.

Ключевые слова: цифровые компетенции, цифровая трансформация, цифра, организация, цифровые технологии, цифровые инструменты, сотрудник

DEVELOPMENT OF DIGITAL COMPETENCIES OF EMPLOYEES IN ORGANIZATIONS UNDERGOING DIGITAL TRANSFORMATION

Abstract. The article discusses the digital competencies necessary for successful work in the modern world. The author describes the main aspects of digital competencies: efficiency, innovation, flexibility, responsibility and self-development. The problems in the formation of digital competencies in the organization are considered. It also provides a list of organizational measures that contribute to the increment of the company's digital capital.

Keywords: digital competencies, digital transformation, digit, organization, digital technologies, digital tools, employee

Окружающий мир, который раньше был относительно простым и предсказуемым, постепенно становится все более изменчивым, сложным и неоднородным. По результатам исследования, проведенного среди населения планеты, 79 % респондентов считают, что изменения происходят слишком быстро и непредсказуемо [1. С. 36].

Континуум современной экономики характеризуется динамичными изменениями. Важным фактором производства становится не земля или капитал, а че-

ловек с его знаниями и новым мышлением, формирующимся в результате этих изменений.

Оптимизация экономических процессов, основанная на современных достижениях, привела к тому, что человек стал играть важную роль в решении многих задач в различных отраслях экономики. Ученые из Университета Дикина считают, что на смену «Индустрии 4.0» с ее автоматизацией приходит «Индустрия 5.0», которая предполагает возврат внимания к человеку, учет его психофизиологических, когнитивных и поведенческих особенностей, а также объединение человеческого интеллекта и творческих способностей с возможностями машин и технологий [2. С. 711].

К целям конвергенции цифровых технологий и человеческого фактора в рамках организационного пространства можно отнести следующее:

– повышение эффективности производственных и экономических процессов с высокой добавленной стоимостью;

– оптимизацию взаимодействия человека и машин;

обеспечение свободного и равного функционирования сотрудников в организационной среде;

– создание новой внутренней системы с возможностью интеграции в цифровую внешнюю среду;

– возможность совместного использования ресурсов;

– формирование цифровой среды на основе открытых принципов;

– обеспечение физической, личной, интеллектуальной и технологической безопасности;

– преобразование глобальных цепочек потребительской ценности.

Результатами синтеза цифровых технологий и навыков сотрудников могут выступать следующее:

1. Цифровые решения могут помочь работникам автоматизировать рутинные и операционные задачи, что позволяет сосредоточиться на более сложных и творческих задачах, приводит к сокращению времени на выполнение стратегических целей. Это может привести к повышению производительности и улучшению качества работы.

2. Улучшение коммуникации и координации в компании. Цифровые инструменты улучшают коммуникацию между работниками и руководством, а также упрощают координацию между различными отделами и командами.

3. Улучшение обучения и развития – цифровые инструменты могут помочь работникам получить доступ к новым знаниям и навыкам, что способствует их развитию и росту.

4. Использование цифровых технологий снижает затраты на производство и обслуживание оборудования, а также уменьшает количество ошибок и дефектов в работе.

5. Улучшение экологической устойчивости. Цифровые технологии способствуют уменьшению выбросов вредных веществ и снижению энергопотребления, что является важным аспектом экологической устойчивости.

Технологическая трансформация организации, влияя на внутренние ценностные ориентиры, изменяет корпоративную среду и установки, затрагивающие

аспекты трудовых взаимоотношений и лидерства. С учетом личностной идентичности, командной приверженности, стремления к новому, обучению и профессиональному развитию, ответственности и других составляющих сотрудников выстраивается новая система координат. Формирование навыка понимания своего места в цифровых итерациях и способность экологично достигать целей становятся ключевыми критериями эффективной работы в цифровой организационной культуре.

При этом следует отметить определенные проблемы формирования цифровых компетенций:

1. Недостаток информации и знаний о цифровых технологиях: многие люди не имеют достаточного понимания о том, как работают цифровые технологии и как они могут быть использованы в повседневной жизни.

2. Недоступность цифровых ресурсов: некоторые люди могут жить в регионах, где нет доступа к высокоскоростному Интернету или другим цифровым ресурсам.

3. Недостаточное время для обучения: у многих людей есть другие обязательства, такие как работа, семья и учеба, которые могут мешать им уделять достаточно времени обучению цифровым технологиям.

4. Негативные стереотипы о технологиях: некоторые люди считают, что технологии только усложняют жизнь и не приносят никакой пользы.

5. Негативный опыт использования технологий: если у человека был негативный опыт использования цифровых технологий, например, из-за ошибок или сбоев, это может повлиять на его отношение к технологиям в целом.

Развитие цифровых компетенций сотрудников предполагает реализацию корпоративных задач с помощью общих и комплементарных цифровых навыков. При этом функциональные обязанности могут выполняться и за пределами места нахождения работодателя. Навыки дистанционной работы становятся все более ценным ресурсом в цифровом мире

По мнению В. А. Сухомлина, Е. В. Зубаревой и А. В. Якушина, существуют следующие цифровые навыки:

1. Общеупотребимые – помогают ориентироваться и адаптироваться к современным информационным технологиям, с которыми сталкивается человек в повседневной деятельности. С возрастом такие навыки даются с большим трудом.

2. Комплементарные – навыки, которые способствуют решению определенных задач. Зачастую последние соотносятся с деятельностью на рабочем месте. Информационные технологии, которые присутствуют в рабочем процессе, требуют определенной подготовки и умения. Например, коммуникации с коллегами и клиентами могут быть выстроены на базе мессенджеров и корпоративных сетей, а платформы электронной коммерции могут быть непременным атрибутом управления дистрибуторскими потоками, помимо прочего в компании могут быть инструменты аналитики больших данных, бизнес-планирование и пр.

3. Профессиональные – это более сложные навыки цифрового мышления, которые проявляются в умении программирования, проектирования, написания кода и приложений, а также управления большими массивами информации и др.

4. Проблемно-ориентированные – это надстроечные навыки формирования цифровых экосистем, правил и процедур информационного обмена, цифровых платформ, систем и программ, позволяющих формировать уникальный цифровой код компании [3. С. 148].

Работа в цифровой компании дают человеку неоспоримые преимущества: высокий спрос на рынке труда, быстрый вход в профессию, подходит людям в зрелом возрасте, высокие зарплаты и пр.

Оценку эффективности цифровой трансформации предприятия можно оценить по изменению управляемости персонала после проведенных мероприятий по цифровизации. Предполагается, что проведение цифровой трансформации опосредованно будет влиять на следующие параметры:

– удовлетворенность организацией труда;

– удовлетворенность уровнем механизации и автоматизации труда;

– удовлетворенность уровнем собственной квалификации;

– удовлетворенность содержанием своего труда, возможностью самореализации;

– увеличение привлекательности работы в институте по позиции «творческое начало в работе (интеллектуальный рост, самореализация, интересная работа)».

Список литературы

1. Безуглова М. Wellbeing как ДНК корпоративной культуры // Business Excellence. 2020. № 5. С. 34-39.

2. Brunetti F., Matt D. T., Bonfanti A., De Longhi A., Pedrini G., Orzes G. Digital Transformation Challenges: Strategies Emerging from a Multi-Stakeholder Approach // The TQM Journal. 2020. Vol. 32, № 4. Pp. 697-724.

3. Сухомлин В. А., Зубарева Е. В., Якушин А. В. Методологические аспекты концепции цифровых навыков. Современные информационные технологии и ИТ-образование. 2017. Т. 13, № 2. С. 146-152.

И. И. Коверченко,
ассистент кафедры,
Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации
(Волгоградский институт управления – филиал РАНХиГС)

ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПЛАТФОРМЕННОЙ ЗАНЯТОСТИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОПЫТА РОССИИ И ЗАРУБЕЖНЫХ СТРАН

Аннотация. Стремительное развитие гиг-экономики оказало сильное влияние на трудовые отношения в современном мире. Благодаря появлению такого инструмента, как цифровые платформы, работники получили уникальную возможность оказывать услуги, при этом фактически сохраняя значительную долю

самостоятельности и независимости относительно классической трудовой занятости. Однако возможно ли рассматривать отношения между работником и компанией – владельцем платформы с точки зрения классического трудоустройства, или все же это уникальное явление? Для ответа на данный вопрос в статье будут приведены варианты правового регулирования трудоустройства гиг-работников на цифровых платформах в различных странах. Исследование выполнено за счет гранта Российского научного фонда № 22-28-00914.

Ключевые слова: гиг-экономика, цифровые платформы, платформенная занятость, гиг-работники, платформенные работники, micro-entrepreneurs, ZZPer

LEGAL REGULATION OF PLATFORM EMPLOYMENT: A COMPARATIVE ANALYSIS OF THE EXPERIENCE OF RUSSIA AND FOREIGN COUNTRIES

Abstract. The rapid development of the gig economy has had a strong impact on labor relations in the modern world. In particular, thanks to the emergence of such a tool as digital platforms, employees have received a unique opportunity to provide services while actually maintaining a significant amount of autonomy and independence relative to classical employment. However, is it possible to consider the relationship between the employee and the company that owns the platform from the point of view of classical employment, or is it still a unique phenomenon? To answer this question, the article will provide options for the legal regulation of the employment of gig workers on digital platforms in various countries.

Keywords: gig economy, digital platforms, platform employment, gig workers, platform workers, micro-entrepreneurs, ZZPer

На сегодняшний день практически каждый гражданин так или иначе взаимодействует с цифровыми платформами, будь то оплата и доставка товаров, заказ такси, клининговые услуги и т. п. Благодаря появлению цифровых платформ, взаимодействие между заказчиком и исполнителем становится максимально удобным и быстрым. При этом стоит заметить, что платформенная занятость – явление достаточно новое, так как оно непосредственно связано с развитием гиг-экономики. В связи с этим, в России, как и в большинстве зарубежных стран, все чаще на обсуждение стал выноситься вопрос о соответствии законодательства современным тенденциям, которые задаются платформенным трудоустройством. Действительно, работники цифровых платформ представляют собой неклассический пример занятости – начиная от нормирования рабочего времени и заканчивая режимом налогообложения. Крупные цифровые платформы предпочитают использовать работников в краткосрочный период посредством заключения гражданско-правовых договоров, поскольку это значительно снижает их издержки [3. С. 266].

В большинстве стран на данный момент не существует единого подхода к оформлению платформенных работников. Противоречия, как правило, исходят из самой сути деятельности гиг-работников – кто-то считает их самозанятыми (например, такой подход характерен для России и Франции [10. P. 19]), а где-то до-

пускается их трудоустройство по классической схеме – как полноценных сотрудников (например, в Германии [5. С. 23] или Швеции [5. С. 35]). Большое влияние на выбор того или иного подхода оказывает количество платформенных занятых в стране. Действительно, учитывая тенденцию роста популярности работы в подобном формате, неудивительно, что все большее количество стран не просто обращают внимание на данную проблему, но и организуют разнообразные научные мероприятия и конференции, в рамках которых ведущие специалисты, практики и ученые могут высказать свое мнение и предложить свою модель развития платформенного законодательства.

Так, в России платформенная занятость регулируется Трудовым и Налоговым кодексами, а также рядом иных нормативных правовых актов, например, Федеральным законом «О проведении эксперимента по установлению специального налогового режима Налог на профессиональный доход» от 27.11.2018 № 422-ФЗ, поскольку самозанятость является одной из наиболее удобных форм осуществления взаимодействия с платформами как для самих самозанятых (например, отсутствие необходимости в подаче налоговой декларации [7]), так и для владельцев платформ. Стоит также отметить, что большое количество стран отдает предпочтение квалификации платформенных работников в качестве самозанятых, нежели штатных сотрудников.

Российские гиг-работники могут взаимодействовать с платформами в трех режимах:

1) как индивидуальный предприниматель;

2) как самозанятый [6. С. 6];

3) как физическое лицо по договору ГПХ.

Здесь стоит отметить, что на сегодняшний день в законодательстве отсутствует определение платформенной занятости. Так, например, в законопроекте № 275599-8 «О занятости населения в Российской Федерации» в п. 4 ст. 2 под платформенной занятостью считают «деятельность граждан (платформенных занятых) по личному выполнению работ и (или) оказанию услуг на основе заключаемых договоров, организуемая с использованием информационных систем (цифровых платформ занятости), обеспечивающих взаимодействие платформенных занятых, заказчиков и операторов цифровых платформ занятости посредством информационно-телекоммуникационной сети Интернет» [1]. Исходя из данного определения, можно поставить вопрос о включении в перечень платформенных занятых ИП. Вместе с тем приведенная выше классификация основывается на понимании платформенной занятости как по сути любого взаимодействия лиц и платформ, результатом которого является оказание услуг или выполнения определенных работ. В большом количестве современных стран существует проблема с определением термина «платформенная занятость», поэтому в рамках статьи оно будет рассмотрено в широком смысле.

Рассмотрим особенности данных форм. При выполнении работ как самозанятым, так и ИП (по договору ГПХ) или физическим лицом, при оплате труда не учитывается требование о соответствии МРОТ. Налоги уплачиваются согласно выбранному статусу – самозанятые уплачивают налог на профессиональный

доход, ИП платят на общей системе налогообложения НДФЛ, НДС и страховые взносы (при этом ИП могут находиться на одном из специальных налоговых режимов: УСН, НПД, патентная система налогообложения). Для физических лиц также предусмотрена уплата НДФЛ, который удерживается платформой.

Одним из наиболее обсуждаемых вопросов платформенной занятости – особенности социального и пенсионного обеспечения гиг-работников. Так, для самозанятых граждан – плательщиков НПД уплата страховых взносов на пенсионное и социальное страхование не является обязательным. Граждане могут добровольно производить отчисления в Пенсионный фонд РФ и Фонд социального страхования РФ путем заключения договоров [2. С. 324]. ИП уплачивает страховые взносы, за исключением случая, когда он является плательщиком НПД (на данном режиме страховые взносы уплачивать не требуется). Если физическое лицо является исполнителем по договору ГПХ, за него организацией, т. е. платформой, уплачиваются страховые взносы.

Таким образом, в России к платформенным работникам могут применяться положения о социальном и пенсионном обеспечении, что уже является достаточно хорошим знаком, поскольку в некоторых странах гиг-работникам не предоставляется ни социальное, ни пенсионное обеспечение ввиду неоднозначности их трудового статуса с точки зрения закона. Вместе с тем многие стейкхолдеры придерживаются позиции, что посредством трудового договора регулировать платформенную занятость не получится, поскольку не видят в ней разновидность классических трудовых отношений в целом. При этом, по их мнению, не следует менять положения трудового кодекса, в свою очередь имеет смысл разработать самостоятельное государственное регулирование конкретно для данной сферы [6. С. 54–57].

В свою очередь по пути закрепления платформенной занятости в рамках трудового законодательства пошла Франция. Так, гиг-работники могут работать в статусе «Микропредпринимателей» (англ. micro-entrepreneurs) [10. P. 19]. Во Франции периодически принимаются поправки к Трудовому кодексу (фр. Code du travail), в рамках которых расширяется защита прав платформенных занятых [9]. Например, теперь самозанятые работники транспортных платформ получили право доступа к данным, связанным с их трудовой деятельностью [4. С. 26]. Аналогично в Трудовой кодекс Франции были внесены дополнения, касающиеся коллективных действий платформенных работников. Такие поправки предоставили работникам право на коллективные действия, защищая их при этом от ответных мер со стороны платформ (например, от расторжения договора). При этом поправками предусматривается право на объединение и на «отстаивание коллективных интересов» через профсоюзы (фра. faire valoir par son intermédiaire leurs intérêts collectifs) [4. С. 213].

Также уникальной особенностью французского регулирования платформенной занятости является предоставление работникам «права на отключение» (например, от электронной почты или мессенджеров, в том числе от программ, которые обеспечивают выполнение рабочей функции, после окончания рабочего дня) и меры, позволяющие самозанятым работникам платформы добиваться назначения «достойной цены» за работу [5. С. 26].

Особенностей налогообложения в отношении платформенных занятых во Франции не предусмотрено, в связи с чем они платят налоги согласно обычным налоговым ставкам.

Таким образом, Франция выступает одной из наиболее интересных стран с точки зрения правового регулирования платформенной занятости. Благодаря осознанию того, что на сегодняшний день такая занятость обретает все больший объем, законодатель принял решение постепенно дополнять уже существующую правовую систему, вместо того чтобы придумывать кардинально новый режим занятости. Такой подход видится логичным и, что немаловажно, стабильным, поскольку постепенная модернизация законодательства позволит в дальнейшем вывести самую удобную формулу занятости, которая будет полноценно защищена в правовом поле.

Иную ситуацию можно наблюдать в Германии. Так, по немецкому законодательству платформенных работников можно рассматривать и как «классических работников» (с соответствующим признанием трудовых отношений), и как самозанятых [5. С. 23]. Преимуществом работы в качестве самозанятого на цифровых платформах является наличие минимальной планки почасовой заработной платы. При этом на другой чаше весов видится существенный минус – законы о социальном и пенсионном обеспечении распространяются в основном на штатных работников. Более того, законы о защите здоровья и безопасности труда не распространяются на самозанятых. При этом признание самозанятого на платформе в качестве работника видится достаточно проблематичным, и одним из самых действенных способов это сделать является судебная практика. Например, в деле 9 AZR 102/20 работнику удалось добиться признания трудовых отношений и, следовательно, статуса работника платформы [8].

Большую роль в защите прав платформенных занятых в Германии играют профсоюзы. Из самых известных можно отметить такие, как IG Metall, Ver.di, IG BAU и др. Несмотря на явные противоречия в части правового регулирования платформенных занятых, немецкая судебная практика вполне может склониться в пользу гиг-работников и предоставить им статус «классических работников» платформы, поскольку зачастую они просто не могут получить соответствующей правовой защиты в рамках статуса самозанятого.

Таким образом, в Германии пока что отсутствует какое-либо единство относительно законодательного закрепления платформенной занятости. Большую роль в этой стране на сегодняшний день играет судебная практика, поскольку она позволяет гиг-работникам защищать свои права и социальные гарантии, что при отсутствии должного правового регулирования является одним из самых эффективных инструментов. Однако это не значит, что в Германии не признают платформенную занятость как феномен, наоборот, в научной среде ведутся горячие споры по этой теме. И все же результаты таких дискуссий пока что находятся на теоретическом уровне.

Необычным видится подход к правовому регулированию платформенной занятости в Нидерландах. Отличительной особенностью данного правопорядка является наличие уникального вида занятости – «Самозанятые без собственных ра-

ботников» (нид. Zelfstandige Zonder Personeel, или сокращенно ZZPer). По общему правилу, самозанятый выполняет работы согласно заключенному контракту, в том числе с учетом указанной в нем стоимости. Стоит отметить, что Правительство Нидерландов хотело ввести минимальную оплату труда для самозанятых, но в дальнейшем отказалось от этой идеи [15].

ZZper платят подоходный налог и социальное обеспечение через свою годовую налоговую декларацию, а также 21% НДС. При этом стоит иметь в виду, что в Нидерландах действует ограничение на организацию и вступление в профсоюзы. Дело в том, что в некоторых странах платформенные занятые, которые являются независимыми подрядчиками, не могут вступать или создавать профсоюзы. Это связано с тем, что такие объединения могут быть признаны европейским законодательством незаконным картельным сговором [5. С. 52].

При этом судебная практика отнесения гиг-работников к «классическим работникам» или самозанятым достаточно противоречива. Так, в деле с участием крупной платформы Deliveroo суд г. Амстердама пришел к выводу, что правоотношения между платформой по доставке еды и курьером нельзя отнести к категории «работодатель – работник» и, следовательно, такие отношения следует квалифицировать как самозанятость [12]. Обратное решение было принято судом в 2019 году с участием все той же платформы. Так, суд отметил, что курьеры – доставщики еды не являются самозанятыми без собственных работников (ZZPer), и их стоит квалифицировать в качестве сотрудников [11].

Нидерланды аналогично Франции решили пойти по пути развития уже существующих форм занятости. Выбрав наиболее подходящую форму, страна предпринимает попытки по актуализации законодательства, выработке соответствующей судебной практики и т. п. Однако результаты все же оставляют желать лучшего – судебная практика до сих пор не определилась в выборе подхода, при этом в случае осуществления деятельности в качестве ZZPer лицо лишается возможности прибегнуть к такому инструменту, как профсоюз, который во многих странах оказывает значительное влияние на развитие платформенной занятости.

Пожалуй, один из самых прогрессивных подходов на сегодняшний день можно наблюдать в Индии. Принятый в 2020 году Кодекс социального обеспечения (англ. The Code on Social Security) закрепляет два вида платформенной занятости:

1) гиг-работники;

2) платформенные работники [13].

Под гиг-работником понимается лицо, которое, по сути, выполняет работу или оказывает услуги вне формата традиционных трудовых отношений [6. С. 28]. В свою очередь, платформенные работники отличаются тем, что осуществляют свою деятельность путем взаимодействия с соответствующими цифровыми платформами. Для обеспечения социальных гарантий данных категорий работников Кодекс предусматривает создание федерального и региональных фондов социального обеспечения.

Наиболее прогрессивным в Индии оказался штат Раджастан, который стал известен благодаря принятию особого закона – The Rajasthan Platform-Based Gig Workers (Registration and Welfare) Bill, 2023 [14]. Данный закон произвел насто-

ящий фурор в информационном поле, ему было посвящено множество статей в СМИ. Основными нововведениями в рамках данного закона были:

1) принятие налога в размере до 2 % с доходов, полученных цифровыми платформами, работающими в данном штате;

2) создание совета по социальному обеспечению гиг-работников, в состав которого войдут представители правительства штата, работников, платформенных компаний и гражданского общества. Совет будет наделен рядом полномочий, среди которых: курирование фонда социального обеспечения, регистрация работников и цифровых платформ, следить за соблюдением требований законодательства, содействовать предложенным мерам социального обеспечения и др.

По сути, главной целью закона является расширение социальных льгот и гарантий на категорию платформенных работников, что является действительно уникальным опытом не только в Индии, но и в мире.

При этом в Индии все же есть свои существенные проблемы. Так, для платформенных работников по общему правилу предусмотрена планка минимальной заработной платы, в том числе нет положений о выплате премий, отсутствуют какие-либо выходные пособия и пр. Это дает понять, что несмотря на серьезные намерения предоставить гиг-работникам возможность быть наравне (или, по крайней мере, иметь хотя бы часть преимуществ «классических работников») с обычными сотрудниками, Кодекс выступает лишь первым этапом трансформации правовой системы, которая в дальнейшем, хочется верить, и дальше пойдет по пути защиты прав в сфере платформенной занятости. Стоит признать, что подход Индии является достаточно новым и оригинальным, и в ближайшем будущем будет интересно наблюдать эффективность его применения.

Подводя итоги, можно увидеть, насколько разнообразны подходы к регулированию платформенной занятости на сегодняшний день. Если обобщить все вышесказанное, можно сделать вывод, что в большинстве стран дискуссия ведется между двумя позициями – квалификация платформенных работников как работников по стандартному трудовому договору с соответствующим предоставлением всех правовых и социальных гарантий, либо как самозанятых, которые лишены большого количества преимуществ «классической занятости», но при этом более гибки в плане рабочего графика, оплаты труда и т. п. и, следовательно, удобны для найма с точки зрения владельцев цифровых платформ. В некоторых странах пытаются внедрить уникальный, третий путь, который должен учитывать особенности платформенной занятости и при этом давать соответствующее социальное обеспечение и правовую защиту, должного уровня которых, как правило, лишены обычные самозанятые. При решении вопроса о выведении наиболее эффективной формулы платформенной занятости следует учитывать большое количество разнообразных факторов, таких как особенности законодательной системы в конкретной стране, порядок ее функционирования, сложившаяся судебная практика и, конечно, мнение самих гиг-работников и цифровых платформ. При таком раскладе каждое государство стремится в первую очередь разработать такой вариант, который будет удобен в данной конкретной стране. Однако, если обратить внимание на опыт других стран, это позволит увидеть эффективность того или иного

подхода, что в дальнейшем поможет избежать лишних ошибок при модернизации правовой системы.

В любом случае решение вопроса определения правового статуса платформенных занятых является серьезным шагом в развитии гиг-экономики в любой стране. Количество платформенных работников растет с каждым днем, равно как и количество самих цифровых платформ, в связи с чем, поставленная проблематика будет актуальна и требует внимания и обсуждения со стороны как ученых-правоведов, так и практиков в сфере платформенной занятости.

Список литературы

1. Законопроект № 275599-8 «О занятости населения в Российской Федерации» / Система обеспечения законодательной деятельности Государственной автоматизированной системы «Законотворчество» (СОЗД ГАС «Законотворчество»). URL: https://sozd.duma.gov.ru/bill/275599-8.

2. Миронова С. М., Кожемякин Д. В., Пономарченко А. Е. Адаптация правового регулирования трудовых, гражданских, налоговых правоотношений к условиям гиг-экономики // Правоприменение. 2022. № 4. С. 323-324.

3. Миронова С. М. Правовая природа и роль цифровых платформ в условиях гиг-экономики / С. М. Миронова // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции. В 6 т., Казань, 23 сентября 2022 г. / под ред. И. Р. Бегишева [и др.]. Т. 1. Казань: Познание, 2022. С. 264-275.

4. Перспективы занятости и социальной защиты в мире. Роль платформ цифрового труда в трансформации сферы труда, 2021 / Группа технической поддержки по вопросам достойного труда и Бюро МОТ для стран Восточной Европы и Центральной Азии. М.: МОТ, 2021. 283 с. URL: https://www.ilo.org

5. Платформенная занятость: вызовы и возможные решения / Фонд «Центр стратегических разработок» (ЦСР). М., 2022. 71 с.

6. Платформенная занятость: определение и регулирование (2021) / О. В. Синявская, С. С. Бирюкова, А. П. Аптекарь, Е. С. Горват, Н. Б. Грищенко, Т. Б. Гудкова, Д. Е. Карева; Национальный исследовательский университет «Высшая школа экономики», Институт социальной политики. М.: НИУ ВШЭ, 2021. 78 с.

7. Федеральный закон от 27.11.2018 № 422-ФЗ «О проведении эксперимента по установлению специального налогового режима «Налог на профессиональный доход» // Российская газета. 2018. № 270(7733).

8. Bundesarbeitsgericht/Federal Labour Court. (2020, Dec 1). Case 9 AZR 102/20. URL: https://www.bundesarbeitsgericht.de/entscheidung/9-azr-102-20/?highlight=9+AZR+102%2F20

9. Code du travail / Légifrance. URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006072050/

10. de Groen, W. P., Kilhoffer Z., Lenaerts K., Mandl I. Employment and working conditions of selected types of platform work / W. P. de Groen, Z. Kilhoffer, K. Lenaerts, I. Mandl; Eurofound. Luxembourg: Publications Office of the European Union, 2018. 86 pp.

11. Rechtbank Amsterdam (2019a). Zaak Deliveroo / FNV, zaaknummmer 7044576 CV EXPL 18-14763, vonnis 15 januari 2019. URL: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2019:198

12. Rechtbank Amsterdam. Zaak Deliveroo / S. Ferwerda, zaaknummmer 6622665 CV EXPL 18-2673, vonnis 23 juli 2019. URL: https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2018:5183

13. The Code on Social Security, 2020 / Правительство Индии. Официальный сайт Министерства труда и занятости. URL: https://labour.gov.in/sites/default/files/ss_code_gazette.pdf

14. The Rajasthan Platform-Based Gig Workers (Registration and Welfare) Bill, 2023. URL: https://www.medianama.com/wp-content/uploads/2023/07/20-06-2023FinalDraftofPBGWWBill2023byLawDepartment.pdf

15. Zzp'ers gaan vanaf 2021 minimaal 16 euro per uur verdienen / Официальный сайт Правительства Нидерландов. URL: https://www.rijksoverheid.nl/actueel/nieuws/2019/06/24/zzp%E2%80%99ers-gaan-vanaf-2021-minimaal-16-euro-per-uur-verdienen

Н. А. Курьянов,
соискатель,
Ташкентский государственный юридический университет

ОТРАЖЕНИЕ РАЗЛИЧНЫХ АСПЕКТОВ ЦИФРОВИЗАЦИИ ТРУДОВЫХ ОТНОШЕНИЙ В НОВОМ ТРУДОВОМ КОДЕКСЕ РЕСПУБЛИКИ УЗБЕКИСТАН

Аннотация. Цель статьи заключается в анализе влияния процессов цифровизации на систему трудовых отношений в Узбекистане и отражении обусловленных ими трансформационных изменений в Трудовом кодексе Республики Узбекистан. Отмечается, что принятие имеющей концептуальное значение для долгосрочного развития государства стратегии «Цифровой Узбекистан – 2030», а также рост удаленной занятости в условиях пандемии COVID-19 обусловили необходимость формирования системы законодательного регулирования подобной формы организации трудовых отношений. Достаточно подробно рассмотрен широкий спектр положений, регулирующих различные аспекты дистанционной занятости, которые были внесены в новый Трудовой кодекс Узбекистана, вступивший в силу в апреле 2023 года. Также представлены наиболее актуальные направления совершенствования национального трудового законодательства для учета меняющейся динамики рынка труда в эпоху цифровых технологий.

Ключевые слова: трудовые отношения, цифровизация, дистанционная занятость, пандемия COVID-19, правовое регулирование, Республика Узбекистан, Трудовой кодекс

REFLECTION OF VARIOUS ASPECTS OF DIGITALIZATION OF LABOR RELATIONS IN THE NEW LABOR CODE OF THE REPUBLIC OF UZBEKISTAN

Abstract. The purpose of the article is to analyze the impact of digitalization processes on the system of labor relations in Uzbekistan and reflect the transformational changes caused by them in the Labor Code of the Republic. It is noted that the adoption of the strategy "Digital Uzbekistan-2030", which has conceptual significance for the long-term development of the state, as well as the growth of remote employment in the conditions of the COVID-19 pandemic, necessitated the formation of a system of legislative regulation of such a form of organization of labor relations. A wide range of provisions regulating various aspects of distance employment, which were introduced into the new Labor Code of Uzbekistan, which entered into force in April 2023, has been considered in sufficient detail. The most relevant areas of improvement of national labor legislation to take into account the changing dynamics of the labor market in the digital age are also presented.

Keywords: labor relations, digitalization, remote employment, COVID-19 pandemic, legal regulation, Republic of Uzbekistan, Labor Code

Одной из важнейших тенденций последнего десятилетия, характеризующих направленность социально-экономического развития Узбекистана, с полным правом можно назвать активизацию процессов цифровой трансформации, которые затрагивают практически все сферы жизни государства и общества.

В рамках этих процессов осуществляется внедрение новых информационных технологий в сферы государственного управления, здравоохранения, образования, финансов, транспортного обслуживания и т. д.

Реализуемые в республике мероприятия по развитию цифровой экономики предполагают создание цифровых кластеров, электронных торговых площадок, упрощенной системы онлайн-регистрации бизнеса, а также других мер, направленных на поддержку IT-индустрии и развитие широкого спектра цифровых услуг. При этом их координация базируется на положениях соответствующих стратегически ориентированных документах, принятых на государственном уровне.

В частности, в январе 2019 года был издан Указ Президента Республики Узбекистан «О дополнительных мерах по дальнейшему развитию экономики и повышению эффективности экономической политики, предусматривающий разработку стратегии «Цифровой Узбекистан – 2030», направленный на развитие национальной цифровой экономики. В октябре 2020 года Ш. Мирзиеев соответствующим Указом утвердил данную стратегию и обозначил основные направления ее реализации [2].

Стратегия «Цифровой Узбекистан – 2030» определяет основные ориентиры и механизмы реализации национальной политики в области обеспечения цифровой трансформации на ближайшие годы и включает в себя широкий комплекс мер по совершенствованию информационной инфраструктуры, расширению цифрового образования населения, развитию блокчейн-технологий и других важнейших аспектов цифровой экономики [9. С. 136].

В рамках реализации данной стратегии предполагается осуществление цифровой трансформации, с одной стороны, регионов, а с другой – отдельных индустрий национального хозяйства.

Среди ключевых направлений реализации указанной стратегии отмечены развитие электронного правительства, системы предоставления цифровых услуг для граждан и бизнеса, цифрового образования, цифровой инфраструктуры, национального рынка цифровых технологий, цифровых навыков как элемента человеческого капитала, а также эффективных систем защиты информации.

Пои этом предполагается повышение доли охвата населения подключением к Интернету до 95%, внедрение национальной системы ID-карт для граждан, существенное увеличение протяженности оптоволоконных линий, внедрение новых информационных технологий и электронных услуг.

По программе «Миллион узбекских кодеров» более 600 тысяч человек должны пройти обучение основам компьютерного программирования, а также в 200 профильных школах вводится углубленное изучение информационных технологий.

Таким образом, в Узбекистане поддержка процессов цифровизации на государственном уровне является одним из приоритетных направлений обеспечения стратегического развития национальной экономики и общественной жизни в целом. Государство активно способствует внедрению новых информационно-коммуникационных технологий и стимулирует использование цифровых инструментов в различных сферах деятельности.

При этом подобное развитие ситуации обусловило необходимость внесения существенных изменений и дополнений в нормативную правовую базу Республики Узбекистан в контексте самых разных направлений общественно-экономического развития, которые самым непосредственным образом затрагивают процессы цифровой трансформации. Несомненно, к числу важнейших в ряду этих направлений относится развитие новых форм трудовых отношений, непосредственно связанных с использованием современных цифровых технологий.

Учитывая, что развитие дистанционных форм реализации работников своих трудовых функций имеет место начиная с 2000-х, следует отметить, что катализатором их бурного роста явилась пандемия COVID-19 в 2020 году, вынудившая многие предприятия перевести своих сотрудников на подобный режим работы [10]. Подобная ситуация внесла существенные изменения и в динамику спроса и предложения на рынке труда в отношении услуг, оказываемых в подобной форме.

В частности, в течение первого полугодия 2021 года число размещенных на сайте hh.uz вакансий, которые предполагают осуществление работы в дистанционном формате, превысило показатель за аналогичный период 2020 года в девять раз, а количество заявок от соискателей, которые отметили подобный формат занятости в качестве приоритетного, – в четыре раза [5]. При этом, как показали результаты проведенных узбекскими специалистами эмпирических исследований, организация трудовой деятельности в трудовом формате существенно усложняет процесс управления этим процессом [11. С. 46].

В то же время законодательное регулирование осуществления трудовой деятельности в дистанционном формате на момент проявления пандемийных тен-

денций в Узбекистане отсутствовало. В данном контексте многие специалисты указывали на важность введения норм, регулирующих основные аспекты осуществления работником своих трудовых функций в дистанционном формате, в национальное трудовое законодательство [8. С. 83].

Первым шагом на пути формирования нормативной правовой базы в области регулирования дистанционной занятости в стране стало принятие в марте 2020 года Положения о временном порядке перевода работников на работу в дистанционном режиме работы, по гибкому графику работы или на дому в период действия карантинных мер [4].

В указанном Положении впервые было закреплено определение понятия «дистанционная работа», обозначены права работодателя и работника, исполняющего свои трудовые функции в подобном формате. определен порядок заключения и перечислены условия, закрепляемые в договоре о дистанционной работе, обозначен порядок временного перевода работника на дистанционный формат, а также определен круг работников, обладающих преимущественным правом подобного перевода.

В 2022 году данные положения в расширенном формате обрели свое закрепление в новом Трудовом кодексе Республики Узбекистан, вступившем в действие в апреле 2023 года [1].

Говоря о важнейших сентенциях, имеющих отношение к регулированию дистанционной занятости, следует отметить, что ключевым положением, содержащимся в данном документе, следует признать распространение на дистанционных работников положений трудового законодательства с учетом особенностей, отраженных в тексте Трудового кодекса Узбекистана.

Возможность заключения договора о дистанционной работе предусматривается как в общем порядке, так и с помощью обмена электронными документами. Среди положений, которые должны содержаться в его тексте, выделены регламентация графика дистанционной работы, порядка чередования форматов обычной и дистанционной работы при осуществлении трудовых функций в дистанционном режиме, способы обмена информацией между сторонами трудовых отношений, порядок обеспечения работника оборудованием, необходимым для его трудовой деятельности, и его инвентаризации либо возмещения затрат работника в случае использования им собственного оборудования.

При этом устанавливается, что прием либо переход работника на дистанционную работу должен быть оформлен приказом работодателя.

В Трудовом кодексе Узбекистана определены категории работников, имеющих преимущественное право временного перехода на дистанционный режим осуществления своих трудовых функций в случаях, связанных с проявлением последствий катастроф природного либо техногенного характера. К ним отнесены беременные женщины, родители либо опекуны детей, которым не исполнилось 14 лет, лица с инвалидностью, пенсионеры по возрасту, а также работники, которые осуществляют уход за лицами, нуждающимися в осуществлении ухода за ними.

Также констатируется, что особенности организации труда дистанционных работников, к которым отнесены порядок и сроки их обеспечения необходимым оборудованием и иными средствами, порядок и сроки представления работником отчетов об исполненной им работе, условия выплаты компенсации работникам, использующим в трудовом процессе принадлежащие им либо арендованные технические средства, а также возмещения других расходов, обусловленных выполнением дистанционной работы, должны определяться в коллективном договоре, локальных актах либо соглашении работника и работодателя.

В качестве источников, в рамках которых определяется порядок взаимодействия работодателя и дистанционного работника, определены трудовой договор либо локальный акт, принимаемый по согласованию с профсоюзным комитетом. Ключевым моментом в данном контексте является установление конкретного времени исполнения дистанционным работником своих трудовых функций.

При этом в Трудовом кодексе Узбекистана определено, что также за работником может быть закреплена обязанность реагировать на запросы работодателя, связанные с осуществлением трудовой функции, и конкретные временные рамки, в которые должен поступить ответ работника на подобный запрос. С другой стороны, работник наделяется правом не отвечать на такие запросы за пределами установленного рабочего времени. Также дистанционный работник освобождается от ответственности за отсутствие либо несвоевременность ответа на запрос работодателя в случае неурегулированности сторонами порядка их взаимодействия либо если работник не был ознакомлен с этим порядком. Отдельно отмечается, что процедура подобного ознакомления может быть произведена путем обмена сторон соответствующими электронными документами.

Что касается рабочего времени дистанционного работника, то в Трудовом кодекса Узбекистана в обязанности работодателя вменяется необходимость при формировании рабочего задания учета нормативов времени на выполнение отдельных видов работ, с тем чтобы его общая продолжительность находилась в рамках нормальной продолжительности рабочего времени.

Следует отметить, что предусматривается подразделение рабочего времени дистанционного работника на две категории – фиксированное, в течение которого он должен быть в режиме непосредственного взаимодействия с работодателем, и время, порядок использования которого определяется самим работником. При этом на второй из указанных режимов не распространяется практика оплаты за сверхурочную и ночную работу, а также работу в выходные дни за исключением ряда оговоренных в тексте ТК случаев. Взаимодействие работодателя с работником в нерабочее время допускается в исключительных случаях и подлежит повышенной оплате.

В отношении ежегодного отпуска дистанционных работников устанавливается, что его продолжительность не может быть менее 21 дня, а порядок его предоставления должен определяться в трудовом договоре.

Наконец, касательно оплаты труда дистанционных работников положения Трудового кодекса определяют, что в случае использования повременной системы она осуществляется исходя из отработанного времени, а в случае применения

сдельной системы – из выполненного объема работ в соответствии с нормами выработки и расценками, зафиксированными в трудовом договоре. В данном контексте акцент делается на сопоставимости размеров оплаты труда дистанционного работника и работника, занятого непосредственно на предприятии данного работодателя. При этом ее величина не может быть ниже законодательно установленного размера минимальной оплаты труда.

Совокупность вышеприведенных положений, содержащихся в новом Трудовом кодексе Республики Узбекистан, в общем и целом закладывает достаточно развернутую правовую основу для полноценного обеспечения трудовых прав дистанционных работников.

Анализируя содержательную сторону данного законодательного акта, можно констатировать, что он содержит наиболее подробную трактовку различных аспектов организации дистанционного труда по сравнению с положениями трудовых кодексов других постсоветских государств. В частности, об этом может свидетельствовать тот факт, что данной проблематике посвящены 13 статей Кодекса, что существенно больше, чем в указанных документах.

Среди других аспектов развития процессов цифровизации трудовых отношений, нашедших свое отражение в новом Трудовом кодексе Узбекистана, следует отметить регламентацию статуса электронных трудовых книжек, управление которыми реализуется в рамках межведомственного аппаратно-программного комплекса «Единая национальная система труда». При этом все сообщения об изменении трудового статуса работника вносятся в подобные трудовые книжки в автоматическом режиме.

Однако следует отметить и неурегулированность в рамках Трудового кодекса Узбекистана ряда отношений, связанных с влиянием процессов цифровизации на трудовую сферу. Прежде всего, это касается активного становления такой формы нестандартной занятости, как платформенная.

В частности, одной из ключевых проблем в данном аспекте является юридическое закрепление статуса работников, осуществляющих свою трудовую деятельность с помощью онлайн-платформ, и обеспечение их права на получение набора социальных гарантий.

Например, Yandex Eats («Яндекс.Еда»), оказывающий в Ташкенте услуги по доставке еды из заведений общепита, дистанцируется от отношений найма с курьерами, а регистрация данных отношений осуществляется только на платформе. Таким образом, занимающиеся подобной деятельностью работники не имеют никаких социальных гарантий. С другой стороны, они не исполняют своих обязанностей, связанных с уплатой налогов [6]. То же самое можно сказать и об активно развивающемся с 2018 года в Узбекистане сервисе «Яндекс.Такси».

При этом первые шаги к юридическому закреплению статуса работников, занимающихся подобной деятельностью, в Узбекистане были сделаны в 2021 году. В подписанном Ш. Мирзиеевым Постановлении № ПП-5108 «О мерах по дальнейшему упрощению регулирования деятельности по перевозке пассажиров автомобильным транспортом» индивидуальным предпринимателям была предоставлена возможность оказывать услуги такси через соответствующие платформы-агрега-

торы [3]. В итоге за первые пять месяцев реализации подобного эксперимента регистрацию оформили более 5 тысяч работников, а общая сумма налоговых поступлений от их деятельности составила 2,22 млрд сумов в разрезе фиксированного налога и 3,93 млрд сумов – в разрезе социального налога [7]. В данном контексте, учитывая успешный результат проведения этого эксперимента, представляется вполне целесообразным осуществить юридическое закрепление основных положений, регулирующих деятельность работников, реализующих свои трудовые функции с помощью онлайн-платформ, в национальном законодательстве, в том числе и в Трудовом кодексе Республики Узбекистан.

Таким образом, можно заключить, что стремительное развитие процессов цифровизации, имеющее место в последние годы в Узбекистане, обусловило необходимость формирования соответствующей нормативной правовой базы, ориентированной на обеспечение реализации трудовых прав дистанционных работников. При этом ключевые положения Трудового кодекса Узбекистана, регулирующие данную проблематику, в общем и целом позволяют заложить достаточно устойчивую основу для дальнейшего полноценного развития процессов цифровизации трудовых отношений, что, Однако не отменяет необходимости совершенствования национального трудового законодательства.

Список литературы

1. Трудовой кодекс Республики Узбекистан // Национальная база данных законодательства Республики Узбекистан от 29 октября 2022 г., № 02/22/798/0972. URL: https://lex.uz/ru/docs/6257291

2. Указ Президента Республики Узбекистан № УП-6079 от 5 октября 2020 г. «Об утверждении Стратегии «Цифровой Узбекистан – 2030» и мерах по ее эффективной реализации» // Национальная база данных законодательства, 06.10.2020, № 06/20/6079/1349. URL: https://lex.uz/ru/docs/5031048

3. Постановление Президента Республики Узбекистан № ПП-5108 «О мерах по дальнейшему упрощению регулирования деятельности по перевозке пассажиров автомобильным транспортом» // Национальная база данных законодательства, № 07/21/5108/0453. URL: https://lex.uz/docs/5422738

4. Приказ министра занятости и трудовых отношений Республики Узбекистан № 3228 от 28 марта 2020 г. «О утверждении Положения о временном порядке перевода работников на работу в дистанционном режиме работы, по гибкому графику работы или на дому в период действия карантинных мер. URL: https://lex.uz/docs/4776267

5. Как выросла популярность удаленной работы в Узбекистане и что будет дальше. URL: https://www.spot.uz/ru/2021/08/13/job

6. Как защитить курьеров и водителей такси. URL: https://anhor.uz/society/couriers/?utm_source=rss&utm_medium= vk&utm_referrer=https%3A%2F%2Fvk.com%2F

7. Похоже, на рынке такси Узбекистана Uber-модель прижилась, легализовав более 5 тысяч «леваков». URL: https://xs.uz/ru/post/pokhozhe-na-rynke-taksi-uzbekistana-uber-model-prizhilas-legalizovav-bolee-5-tysyach-levakov

8. Рахимов М. Пандемия: меҳнат қонунчилиги. Ислоҳотларга мухтожми? // Review of Law Science. 2020. № 1. Pp. 82-86.

9. Хамдамова Ф. Стратегия «Цифровой Узбекистан – 2030»: предпосылки для принятия, основные положения, механизмы и перспективы реализации // Жамият ва инновациялар. 2020. № 1.

10. Юлдашева Д., Баширова П. Дистанционная работа в Узбекистане. URL: https://gratanet.com

11. Fayzieva M., Goyipnazarov S., Abdurakhmanova G. Assessing the impact of teleworking on employees. labor productivity and effectiveness of entity in the period of COVID-19 // Society and Innovations. 2020. Iss. 2. P . 35-52.

12. Khozhabekov M. The remote method of organizing the work of workers in Uzbekistan // Review of Law Sciences. 2020. № 2. P . 115-118.

Е. Н. Лавриненко,
старший преподаватель,
Южный федеральный университет

РОЛЬ И РЕАЛИЗАЦИЯ ЦИФРОВИЗАЦИИ В СИСТЕМЕ УПРАВЛЕНИЯ ТРУДОВЫМИ ОТНОШЕНИЯМИ

Аннотация. В статье рассматривается вопрос применения цифровизации как эффективного инструмента в управлении трудовыми ресурсами, необходимость реализации цифровых инструментов в систему управления современной компанией, в частности, цифрового способа отбора кадров. Анализируются тенденции российских компаний в условиях цифровой реальности, такие как сбор данных о соискателях, аналитика и отбор резюме, помощь успешным кандидатам, посредством электронного документооборота при трудоустройстве.

Ключевые слова: право, трудовые отношения, цифровизация, цифровые инструменты, экономика, управление, человеческий капитал

THE ROLE AND IMPLEMENTATION OF DIGITALIZATION IN THE LABOR RELATIONS MANAGEMENT SYSTEM

Abstract. The article discusses the use of digitalization as an effective tool in the management of human resources, the need to implement digital tools in the management system of a modern company, in particular, the digital method of personnel selection. The trends of Russian companies in the conditions of digital reality are analyzed, such as the collection of data on applicants, analytics and resume selection, assistance to successful candidates, through electronic document management during employment.

Keywords: law, labor relations, digitalization, digital tools, economics, management, human capital

В широком смысле под цифровизацией подразумевается научно-технологическая и организационная деятельность по созданию информационно-цифровой инфраструктуры в целях обеспечения эффективного управления, активизация инновационных процессов посредством использования цифровых программных продуктов [1. С. 32–37]. Современные компании функционируют в условиях перехода к полной цифровизации, которая в настоящее время развивается стремительными темпами и динамично трансформирует не только хозяйствующие субъекты, но и экономику в целом [2. С. 82–84]. Цифровая среда открывает новые горизонты для реализации управленческих функций в кадровой работе. Цифровая трансформация в трудовых отношениях имеет свою специфику. Все шире используется процесс диджитализации при подборе персонала, который подразумевает электронные обращения – передачу информации через сеть Интернет – отправка резюме. Такая схема позволяет работодателям отслеживать, выявлять, приглашать кандидатов.

Внедрение цифровых инструментов в кадровую работу подразумевает:

1. Использование электронных систем управления кандидатами для управления заявками и профилями кандидатов, например, Applicant Tracking System (ATS) – комплекс, автоматизирующий процесс рекрутинга и найма, наиболее часто доступное в облаке в варианте SaaS.

2. Внедрение цифровых инструментов для анализа удовлетворенности сотрудников и обратной связи, например, ежегодный опрос сотрудников QWAYBE – платформа для сбора и эффективного анализа обратной связи от сотрудников) – способствует пониманию и лучшему предсказанию рисков текучести кадров. Современные HR-тренды направлены на использование цифровых инструментов и онлайн-опросов, которые позволяют создать опрос и мгновенно преобразовать его в собрание без необходимости регистрации. Это формирует более динамичную трудовую атмосферу.

3. Использование цифровых систем управления обучением (LMS) для поддержки обучения и обучения сотрудников.

4. Использование цифровых инструментов для планирования и проведения встреч и совместной работы в команде. В настоящее время используются инновационная база знаний от российского разработчика TEAMLY, Яндекс. Диск, Яндекс. Телемост.

Но при применении на практике цифрового подбора персонала обнаруживаются отрицательные моменты данного процесса. Так, цифровые технологии не позволяют прогнозировать будущую трудовую деятельность кандидата, это происходит вследствие отсутствия личного участия кандидатов на определенную должность.

Большинство цифровых технологий способствуют управлению персоналом. Например, автоматизация работы с документами (электронный документооборот) упрощает работу кадрового специалиста. Современные методы заставляют прибегать к формам искусственного интеллекта, облегчающим «управление по алгоритму» и «электронный мониторинг эффективности» [3. P. 8].

Цифровая трансформация кадровой работы – это система процессов управления, где ключевым моментом становится управление большими данными (Big Data). Одним из направлений эффективной работы организации является автоматизация процесса труда. В настоящее время многие компании переходят на корпоративные системы учета рабочего времени (Time Control).

Рис. 1. Система учета рабочего времени Time Control

Исходя из своих возможностей, компании выбирают цифровые программы, цифровые платформы и внедряют программные продукты.

Статистическая отчетность в сфере трудовых отношений подразумевает учет трудовых функций граждан цифровых прав трудоспособного населения, а в дальнейшем формирование трудового стажа с правом получения социальных выплат. Из-за роста информационной нагрузки кадровые сотрудники отмечают, что возникает угроза с условиями труда, вследствие этого необходимо создавать соответствующие условия для работы с большими данными, в текущей экономической обстановке нанимателю не всегда удается отследить и обеспечить достойное рабочее место.

В статье представлены теоретические аспекты применения цифровых инструментов в трудовых отношениях, отражающие значительную роль компаний в сфере управления персоналом. Кроме того, рассмотрены потенциальные примеры, открывающиеся с применением цифровых технологий в кадровых процессах. Цифровые технологии все более эффективны во всех областях нашей жизни и трансформируются многие социальными и бизнес-процессами, бизнес-коммуникациями, в том числе и сфера HRM. Они помогают преодолеть в трудовых отношениях рутину повседневности, высвободить человеческие ресурсы для организации других трудовых функций.

Список литературы

1. Кузнецов Н. В., Лизяева В. В. Управление проектами цифровизации: методологический, организационный и финансовый аспекты // Фундаментальные исследования. 2020. № 2. С. 32-37.

2. Лавриненко Е. Н. Цифровые технологии внутрикорпоративного управления в современной компании // Современные проблемы управления в социально-экономических системах: цифровая трансформация экономики, культуры и общества: материалы IV Международной научно-практической конференции, Ростов-на-Дону, 25–28 апреля 2022 года. Ростов-на-Дону: Южный федеральный университет, 2022. С. 82–84.

3. De Stefano V. «Negotiating the algorithm»: automation, artificial intelligence and labour protection // Labour Law Research Network. 2018. № 246. Pp. 8-52.

Н. И. Минкина,
кандидат юридических наук, доцент,
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации

ТРУДОВОЕ ЗАКОНОДАТЕЛЬСТВО РОССИИ: ТЕНДЕНЦИИ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ В ЦИФРОВУЮ ЭПОХУ

Аннотация. В работе представлен авторский обзор тенденций изменения российского трудового законодательства в связи с происходящими в стране процессами цифровизации. Отмечаются некоторые новеллы, проблемные и нерешенные законодателем актуальные вопросы и перспективные направления по дальнейшему совершенствованию Трудового кодекса. Указывается на доработку законодательства в части выстраивания дополнительной защиты персональных данных граждан в потоках электронного обмена информацией и при востребованном использовании разных цифровых платформ, установление новых социальных гарантий в трудовых отношениях, где активно внедряются ресурсы цифровой среды. Сделан итоговый вывод об усилении публично-правовых начал в отечественном трудовом праве и соответственно его защитной функции, а также необходимости расширения пределов государственного управления в сфере труда в условиях его перехода на цифру.

Ключевые слова: цифровые технологии, электронный документооборот, цифровые платформы, трудовое законодательство, проблемы, тенденции развития, модернизация законодательства

LABOR LEGISLATION OF RUSSIA: TRENDS, PROBLEMS AND PROSPECTS OF DEVELOPMENT IN THE DIGITAL AGE

Abstract. This paper presents the author's review of trends in changes in Russian labor legislation in connection with the ongoing processes of digitalization

in the country. Some novelties, problematic and unresolved by the legislator topical issues and promising directions for further improvement of the Labor Code are noted. It is indicated that the legislation should be finalized in terms of building additional protection of personal data of citizens in the flows of electronic information exchange and with the use of various digital platforms in demand, the establishment of new social guarantees in labor relations, where the resources of the digital environment are being actively introduced. The final conclusion is made about the strengthening of public law principles in domestic labor law and, accordingly, its protective function, as well as the need to expand the limits of public administration in the field of labor in the conditions of its transition «to the figure».

Keywords: digital technologies, electronic document management, digital platforms, labor legislation, problems, development trends, modernization of legislation

Введение. В настоящее время многочисленные цифровые технологии с перспективой роста их количества и усложнения неизбежно и прочно окружают жизнь человека труда. Тем временем с 1 июля 2020 г., согласно ст. 75.1 Конституции Российской Федерации, государство гарантирует ему защиту и уважение. Определение в Основном законе роли человека труда в нашем обществе и провозглашение его защиты в цифровую эпоху не вполне достаточно, нужна конкретная соответствующая (по направлениям государственной охраны) правовая регламентация в трудовом законодательстве. Многие действующие инструменты, механизмы и нормы Трудового кодекса Российской Федерации (далее – ТК РФ) в целом нуждаются в обновлении с учетом достижений цифрового развития. Стремительное развитие интеллектуальных систем на сегодняшний день приводит к значительному опережению трудоправовой практики российского законодательства, тем самым актуализируя целый ряд проблем, требующих своего грамотного правового регулирования. Такая ситуация характеризуется тенденцией усиления публично-правовых начал в отечественном трудовом праве и необходимостью расширения пределов государственного управления в сфере труда.

Основная часть. Трудовые отношения и связанные с ними отношения, названные в ст. 1 ТК РФ, на постоянной основе и регулярно претерпевают закономерные процессы «оцифровывания». За последние два года этот вопрос как в целом, так и по его отдельным элементам становился предметом исследований во многих научных трудах, в частности у М. А. Драчук, [1. С. 131–138], Ю. А. Лукониной [4. С. 130–134], И. А. Филиповой [5. С. 7–32] и др. В юридической литературе, в том числе в работах названных ученых, можно проследить разные аспекты происходящих процессов и акцентирование внимания на них, но при этом нужно учитывать постоянное совершенствование законодательства РФ. Последнее позволяет с учетом новелл и изменений законов представить авторский обзор. В своей основе обобщенно и весьма условно такой обзор можно подразделить на следующие основные направления.

Во-первых, это всем известная продолжающаяся тенденция перехода от бумажных документов к их электронным носителям как в отношении документов работника, так и работодателя. Начиная от формирования сведений о трудовой дея-

тельности работников в электронной форме (ст. 66.1 ТК РФ) и введения цифрового документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета (ст. 65 ТК РФ), и выдачи электронного листка временной нетрудоспособности, формирование иных цифровых документов, связанных с работой, а также с 01.09.2023 выдача медицинской книжки работникам в электронной форме на основании приказа Минздрава России № 90н от 18.02.2022 «Об утверждении формы, порядка ведения отчетности, учета и выдачи работникам личных медицинских книжек, в том числе в форме электронного документа». При этом как переходный период, в течение 6 лет действия указанного приказа работники могут получить по личному заявлению такую книжку на бумажном носителе с подписью уполномоченного лица и печатью уполномоченного учреждения.

Нужно заметить, что в каких-то случаях осуществлен полный переход на электронные документы, но в определенных моментах, например, по электронным трудовым книжкам при сохранении ведения ее на бумажном носителе (по желанию граждан) фактически работодателями ведется двойная работа по их заполнению, и вряд ли это облегчило современный кадровый документооборот. Данный переходный период будет связан с поколением жизни людей, и, думается, этот же период времени понадобится для постепенного обеспечения граждан электронными подписями для полноценной цифровой жизни в тех условиях, которые закрепляются в нормативных правовых актах.

Поэтому отмеченная тенденция сопровождается расширением границ в применении цифровых подписей на разных документах. Работодатели при взаимодействии с должностными лицами публичных органов власти, органов контроля и надзора все чаще имеют возможность представлять необходимую документацию в удобном им цифровом формате. Из числа последних изменений: согласно новой редакции ч. 2 ст. 15 Федерального закона «О специальной оценке условий труда» теперь отчет о проведении специальной оценки условий труда принимается в форме электронного документа, подписанного усиленной квалифицированной электронной подписью или усиленной неквалифицированной электронной подписью, сертификат ключа проверки которой создан и используется в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме.

Во-вторых, взаимосвязанное направление с вышеуказанным – это увеличение числа цифровых платформ и их информационно-техническое усиление для взаимодействия посредством них субъектов трудовых и связанных с ними отношений. Такой знаковой в трудовых отношениях стала Единая цифровая платформа в сфере занятости и трудовых отношений «Работа в России» (ст. 16.2 действующего Закона РФ «О занятости населения в Российской Федерации»).

Кроме того, специалистами обосновывается необходимость разработки и внедрения отдельных специальных цифровых платформ, в частности существует проект по созданию Федеральной государственной информационной системы управления охраной труда [3]. Не оспаривая рациональность такого предложения, уместно сразу задаться о возможном резком росте числа создаваемых платформ

в будущем, поэтому целесообразно продумывать их использование в рамках какого-то единого информационного ресурса с соответствующим юридическим закреплением данного вопроса.

Наряду с базовыми информационными системами постепенно становятся востребованными разные подсистемы, например, при формировании медицинской книжки в электронном формате ей присваивается уникальный идентификатор в соответствующей подсистеме, называемой ЭЛМК, и в соответствии с правилами по ведению медицинской документации в форме электронных документов. Другой пример: на официальном сайте Роструда можно в форме электронного документа подавать декларации соответствия условий труда государственным нормативным требованиям охраны труда и здесь же ознакомиться с соответствующим реестром таких деклараций.

Такие информационные ресурсы и цифровые платформы, с одной стороны, стали способом для оперативного обмена информацией между субъектами общественных отношений и их единого хранения с целью удобства выстраивания коммуникаций и повышения мобильности. А с другой стороны, такая цифровая среда выступает средством для выполнения трудовой функции, площадкой для организации рабочего места работника, в том числе при удаленном труде и нетипичных формах занятости. Во втором случае в ближайшем будущем ожидается отдельная правовая регламентация особенностей труда при нестандартной занятости.

Что же касается первого цифрового применения, то на основе ранее проводимых юридических экспериментов с 01.01.2022 вступили в силу положения ст. 22.1–22.3 ТК РФ, в которых предусматривается возможность электронного кадрового документооборота в трудовых отношениях, но пока его использование и выбор цифровой платформы есть право работодателя, реализация которого определяется с учетом императивных требований и условий в этих же нормах. В перспективе предполагается переход на электронное взаимодействие между работником и работодателем (с отдельными установленными законом исключениями дублирования наиболее значимых правовых документов на бумажном носителе) на едином сервисе, где возможно по необходимости организовать государственный и ведомственный контроль и проверку кадровых документов в дистанционном формате. Такая мера в целом будет направлена на стабилизацию трудовых отношений и оформление локальной документации у работодателей в соответствии с законодательными требованиями. Но при этом не исключается появление новых проблем, связанных с расхождением электронных документов с фактически сложившимися трудовыми отношениями и (или) устными договоренностями между сторонами.

В-третьих, наблюдается тенденция к оцифровыванию действий работников и (или) работодателей при реализации их отдельных прав или осуществлении обязанностей, предусмотренных трудовым законодательством. Наглядным примером может послужить новшество, закрепленное в федеральных законах «Об основах охраны здоровья граждан в Российской Федерации» и «О безопасности дорожного движения», которое вступило в силу 01.09.2023. Речь идет о допущении проведения в определенных случаях медицинских осмотров с использованием медицинских изделий, обеспечивающих автоматизированную дистанционную передачу ин-

формации о состоянии здоровья работников и дистанционный контроль состояния их здоровья. Автор предполагает, что ключевым в реализации новой нормы станет следующее установление: при проведении таких осмотров должна быть обеспечена идентификация личности работника, проходящего медицинский осмотр, исключающая прохождение медицинского осмотра иным лицом в соответствии с законодательством. Механизм реализации по идентификации личности в этом случае предстоит выработать с помощью программного оборудования на практике. Пока же, принимая во внимание повышенный уровень опасности работы в области транспорта и сложившуюся объективную реальность по обязательным предрейсовым, послерейсовым медицинским осмотрам в отношении водителей транспортных средств ситуация вызывает у исследователей оправданную тревогу [2. С. 145–147].

В-четвертых, за последние несколько лет в рамках трудовых отношений его субъекты активно используют разнообразные ресурсы цифровой среды. Одним из таких популярных примеров является внедрение работодателем видеонаблюдения. И если на рабочих местах это стало допустимым согласно в ст. 214 и ст. 216.2 ТК РФ, где установлено право работодателя на использование приборов, устройств, оборудования и (или) их комплексов (систем), обеспечивающих дистанционную видео-, аудио- или иную фиксацию процессов производства работ, в целях контроля за безопасностью производства работ и тем самым обеспечение охраны труда работников. Когда же речь идет об установлении системы видеонаблюдения в служебных помещениях, используемых для переодевания и зоны отдыха, то в этом случае суды признают действия работодателя незаконными и недопустимыми (например, в определении Третьего кассационного суда общей юрисдикции от 03.07.2023 № 88-14171/2023). Сказанное позволяет сделать вывод о важности уточнения на законодательном уровне единых требований к порядку реализации и документальному оформлению реализации данного права работодателем, с закреплением запретов, определяющих пределы дозволенного поведения для предупреждения посягательств на конституционные права граждан, связанные с их частной жизнью.

Кроме того, самими работниками с разными целями используются электронные устройства как во время работы, так и после нее по вопросам, связанным с трудом. Продолжительное состояние работников «быть на постоянной связи» с работодателем и его представителями актуализировали еще одну немаловажную проблему: «право работников на отключение», некий «цифровой детокс», с необходимостью строгого ограничения рабочего времени и четким соблюдением времени отдыха трудящихся лиц. И надо заметить, что этот и другой ряд вопросов актуальны не только для российской жизни, но и активно обсуждаются за рубежом [6. С. 123–131].

Заключение. Представляется очевидным, что перечисленные направления трансформации и связанные с ними обозначенные трудоправовые процессы будут со временем только углубляться и интенсивно расширяться. Между тем упомянутые тенденции являются, по сути, констатацией происходящих изменений в реальной жизни, которые пока не по всем вопросам нашли определенную законодательную регламентацию. Представленный обобщенный анализ демонстрирует наличие таких проблем, как необходимость исключения множества юридических коллизий,

касающихся охраны конфиденциальности [4. С. 133] и продуманной государственной защиты персональных данных при использовании различных информационных систем и электронном обмене сведений в трудовых отношениях, безопасного хранения этих данных и усиление контроля со стороны государственных органов за сохранением приватности и обеспечением неприкосновенности частной жизни россиян. Как видно, с распространением цифровой среды в трудовых отношениях актуальность приобретают вопросы по адекватной защите информации.

Наряду с тем, что ожидается непосредственное регулирование новых социальных явлений (к примеру, платформенной занятости в новом Федеральном законе «О занятости населения в Российской Федерации», который пока находится на рассмотрении в Государственной Думе), законодательным органам власти следует комплексно и всесторонне продумать вопрос об установлении новых социальных гарантий работникам и при стандартной (типичной) занятости с целью определения ограничений при использовании различных гаджетов и иных электронных устройств. Это далеко не полный перечень актуальных вопросов, требующих своего законодательного урегулирования. В этой связи представляется очевидной перспектива динамичной модернизации трудового законодательства Российской Федерации в векторе усиления его защитной функции в условиях цифровой трансформации социально-трудовой сферы.

Список литературы

1. Драчук М. А. Цифровизация отношений как вектор государственного управления в сфере труда // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции. В 6 т., Казань, 23 сентября 2022 года / под ред. И. Р. Бегишева [и др.]. Т. 3. Казань: Познание, 2022. С. 131-138.

2. Клепалова Ю. И. Цифровизация медицинских осмотров работников транспорта // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции. В 6 т., Казань, 23 сентября 2022 года / под ред. И. Р. Бегишева [и др.]. Т. 3. Казань: Познание, 2022. С. 143-148.

3. Кузнецова Е. Цифровая трансформация охраны труда. Наше видение перевода всей сферы охраны труда в цифровую плоскость. URL: https://journal.ecostandard.ru/ot/tech/tsifrovaya-transformatsiya-okhrany-truda/

4. Луконина Ю. А. Трансформация трудового права в условиях цифровизации общественных отношений // Актуальные проблемы сравнительного правоведения и юридической лингвистики: материалы Пятой международной научно-практической конференции, Москва, 9–10 декабря 2021 года / ред.: М. Ю. Воронин [и др.]. Москва: Московский государственный лингвистический университет, 2022. С. 130-134.

5. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7-32. EDN LCCOJJ.

6. Шония Г. В. Трудовые отношения во Франции: вопросы цифровизации // Вестник Университета имени О.Е. Кутафина (МГЮА). 2019. № 11(63). С. 123-131.

Е. В. Мотина,
кандидат юридических наук, доцент,
Белорусский государственный университет

ТЕХНОЛОГИИ КОНТРОЛЯ В СИСТЕМЕ ОТНОШЕНИЙ СТОРОН ДОГОВОРА «НОЛЬ ЧАСОВ»

Аннотация. В статье показано расширение возможностей работодателя по контролю над работником в отношениях по предоставлению личного несамостоятельного труда на основе договора «ноль часов». Преимущества договора «ноль часов», как правило, сосредоточены на вопросах экономических выгод, качества работы, баланса работы и личной жизни. Однако расширение контроля, в том числе и за пределы рабочего времени, усиливает личную зависимость работника от работодателя, обостряет и без того неустойчивый характер нетипичных отношений, опосредованных указанным соглашением. Такая дискреционная власть работодателя нарушает пресловутый баланс между работой и личной жизнью, на который обычно указывают как на преимущество выбора такого вида договора для работника. Усложняет положение работников и цифровизация как условие, позволяющее расширить такой контроль, меняя рабочий график в режиме реального времени. Делается вывод о необходимости поиска правового механизма, предусматривающего минимальные компенсации за ограничения прав работников.

Ключевые слова: договор «ноль часов», договор с нефиксированным рабочим временем, нетипичные трудовые отношения, цифровизация, хозяйская власть, контроль над работником, гарантии трудовых прав

CONTROL TECHNOLOGIES IN THE SYSTEM OF RELATIONS BETWEEN THE PARTIES TO A ZERO-HOURS CONTRACT

Abstract. The article shows the expansion of the employer's ability to control the employee in the relationship of providing personal non-self-sufficient labour on the basis of the zero-hours contract. The benefits of a zero-hours contract tend to focus on issues of economic benefits, quality of work, and work-life balance. However, the extension of control, including beyond working hours, increases the employee's personal dependence on the employer, exacerbating the already unstable nature of the atypical relationship mediated by the agreement. Such discretionary power of the employer violates the notorious work-life balance, which is usually pointed out as an advantage of choosing this type of agreement for the employee. Digitalization also complicates the situation of workers as a condition that allows for the extension of such control by changing work schedules in real time. It is concluded that there is a need to find a legal mechanism that provides for minimum compensation for restrictions on workers' rights.

Keywords: zero-hours contract, contract with non-fixed working hours, atypical employment relationships, digitalization, master power, control over the employee, labor rights guarantees

В науке трудового права в последние годы особое внимание уделяется взаимодействию участников наемного труда в условиях цифровизации. Этот феномен изменил и способы выполнения некоторых видов работы по трудовому договору, и способы координации между работниками и работодателями. Цифровизация также способствовала появлению новых форм организации труда, усиливая проблематику так называемых нетипичных трудовых отношений, которые появились до цифровой эпохи и продолжили свое развитие в новых условиях.

Одной из иллюстраций данного тезиса является ни с чем не сравнимое прежде повышение уровня контроля над работниками в процессе трудовой деятельности (например, алгоритмический контроль, контроль на основе искусственного интеллекта (далее – ИИ)) и, как следствие, снижение их автономии, уровня гарантированных прав в рамках трудового правоотношения. Все вместе это является частью общей прекаризации труда. Поэтому полагаем, что не стоит воспринимать все проблемы, порождаемые цифровизацией в сфере труда, как нечто новое и отдельное. Представляется, что распространение так называемых нетипичных трудовых отношений (включая недостаточно четко определенную категорию отношений, опосредованных договором с нулевым рабочим временем (далее – договор «ноль часов», договор с нефиксированным рабочим временем)), ставит перед обществом те же проблемы: прежние механизмы обеспечения прав трудящихся фактически отсутствуют или минимизированы.

Примечательно, что рост числа профессий, основанных на предоставлении услуг, стал ключевой особенностью последних десятилетий. Это еще одна точка соприкосновения цифровизации и нетипичных трудовых отношений, в том числе работы по договору «ноль часов». Важно отметить, что круг профессий, для выполнения работы по которым применяется договор «ноль часов», не ограничивается секторами продаж, уборки, гостиничных услуг, а включает в себя водителей, учителей, воспитателей, бизнес-консультантов и даже преподавателей университетов, архитекторов и инженеров [7]. То есть это вполне традиционные профессии, казалось бы, менее всего подверженные колебаниям экономического спроса. Таким образом, сфера распространения указанного нетипичного договора гораздо шире, чем можно было бы предполагать.

В самом общем виде договор с нулевым рабочим временем может быть определен как вид соглашения о выполнении работы, в соответствии с которым время и продолжительность работы не установлены; работник обязан быть доступным для вызова на работу, выполнять работу в случае предоставления ее работодателем, а работодатель обязан оплачивать труд работника как минимум за фактически отработанное время [2]. Полагаем, что частично эта категория может пересекаться и с другими формами нетипичных трудовых отношений. В частности, с работой, выполняемой через приложения и на основе онлайн-платформ.

При квалификации данных отношений с точки зрения выбора механизмов трудового или гражданского права учитывается принцип контроля работодателя над работником и процессом выполнения работы. Признак контроля относится к организационной составляющей трудового правоотношения. Подчеркнем, что цифровизация способствует развитию новых способов осуществления контроля

над работниками: к его прежним механизмам добавились новые. Это снижает уровень гарантированной автономии работников, усиливает хозяйскую власть работодателя, распространяющуюся, как будет показано, и за пределы трудовых отношений. В литературе высказывается точка зрения, что в условиях гиг-экономики фактически прекратят свое действие наиболее значимые достижения в области трудового права, поскольку «создается сверхгибкий параллельный рынок труда, на котором любые трудовые нормы, считавшиеся до сих пор базовыми, оказываются недостижимыми» [5].

Примечательно, что если раньше исследователи социальной сферы опасались реализации в трудовых отношениях моделей видео- и электронного контроля при организации производственной среды, то в настоящее время уровень опасений снизился. Указанные формы контроля не применяются повсеместно, хотя существующие избыточно наглядные примеры не устают поражать воображение с точки зрения максимального давления на работников. Приведем некоторые примеры. В Китае компания по уборке улиц заставила своих сотрудников носить «умные» браслеты. Они фиксируют режим рабочего времени конкретного сотрудника, а также местоположение дворника в процессе работы. Если браслет не фиксирует телодвижения дольше 20 минут, он отправляет владельцу браслета звуковой сигнал. Если уборщик на него не реагирует, его начальник может отследить координаты браслета и проверить, что происходит с работником [3]. Технологии ИИ контролируют работниц отелей, не только сообщая им, какую комнату убирать, но и отслеживая, как быстро они это делают. Прослушивают работников колл-центра, указывая, что и как они говорят, следя за максимальной занятостью указанных работников [6]. В частности, компания CallMiner рекламирует ИИ, который оценивает вежливость и сочувствие работников колл-центра, измеряемых долей процента. Указанные технологии отслеживают работу разработчиков программного обеспечения, проверяя их клики, прокрутки экрана, фотографируя рабочий стол, и вычитает из общего рабочего времени то, когда работник не производил каких-либо действий, связанных с работой. В итоге продолжительность рабочего дня такого работника увеличивается с 8 до 10 часов, с тем чтобы сохранить оплату труда на прежнем уровне. В некоторых больницах США медсестры носят электронные значки, которые отслеживают, как часто медсестры моют руки [8]. При таком подходе, как справедливо писал И. Я. Киселев, «человек труда для предприятия ничто, лишь выполняемая им функция» [1. С. 9].

Эмпирически установлено, что работники при малейшей возможности стремятся избегать любого цифрового контроля [9], чего нельзя сказать о тех формах контроля, что существуют в отношениях по договору «ноль часов». Под технологиями контроля в системе отношений сторон договора «ноль часов» понимается совокупность методов и инструментов для достижения максимального учета экономических колебаний и параллельно с этим для формирования повышенной дисциплинированности работников, для манипулирования их лояльностью. И если обычно к технологиям применяются требования системности и последовательности, то в рассматриваемом случае их характеристикой является непредвиденность, непостоянство, невозможность провести грань между экономическими и психо-

логическими причинами контроля. Речь идет о возможностях работодателя по установлению непредсказуемого графика рабочего времени в рамках договора «ноль часов».

Современные технологии позволяют корректировать рабочее расписание работников в режиме реального времени. «Свобода работодателей варьировать рабочее время и, следовательно, оплату труда, предоставляет последним широкие полномочия по осуществлению контроля и достижению тех требований, которые не входят в круг обычных трудовых обязанностей» [10] (например, лояльность работника в обмен на предсказуемый рабочий график). Такие практики организационной власти работодателя и контроля на рабочем месте недостаточно изучены в науке трудового права, хотя в антропологических исследованиях названы «гибким деспотизмом», используемым для «наказания» работников [10]. Менеджеры могут «наказывать» работников, не прибегая к традиционным мерам дисциплинарных взысканий. Например, лишить сверхурочных часов, или, наоборот, вопреки прежним договоренностям, вызвать на работу в праздничные дни. Отказ работника чреват дальнейшей потерей рабочих часов, получением только ночных смен и др. Поэтому работники с нефиксированным рабочим временем вынуждены соглашаться на такие изменения. Для них в любом случае это лучше, чем увольнение. При этом доказать такую связь между «наказанием» и изменением графика работы, безусловно, крайне затруднительно.

Кроме многочисленных негативных факторов, сопровождающих выбор описываемой формы занятости, о которых достаточно хорошо известно [2], есть и еще одно обстоятельство. Это повышение зависимости от нанимателя не только на рабочем месте и в рабочее время, но и вне работы. Поскольку работник с нулевым рабочим временем не знает заранее, сколько и когда он будет работать и будет ли вообще. Лишь в некоторых случаях расписание сообщается за месяц или неделю до момента выхода; в других случаях работодатель может вызвать работника за день до того, как работа должна была быть выполнена [2]. Поэтому такую жизнь нельзя назвать автономной, подразумевающей долгосрочное планирование. Работники должны быть постоянно на связи с нанимателем, должны быть готовы ответить на предложение о работе и приступить к ней. Поэтому полагаем, что гибкий график рабочего времени в этих отношениях представляет собой не только способ контроля над работником в рамках рабочего времени, но и за его пределами, а также может выступать в качестве неформальной меры дисциплинарного воздействия [4].

Такой повышенный уровень подчинения делает работников с нефиксированным рабочим временем более уязвимыми для эксплуатации и угрожает ценностям, которые формировались на протяжении столетия и являются центральными в трудовом праве (в частности, речь идет об ограничении хозяйской власти рамками рабочего времени и места работы). Это формирует неподотчетный трудовому праву механизм контроля, расширяя границы организационной и дисциплинарной власти работодателя, усугубляя и без того неустойчивый правовой статус работников с нефиксированным рабочим временем.

При разработке соответствующих правовых норм о договоре с нефиксированным рабочим временем следует учитывать экономическое неравенство сторон договора «ноль часов». Такие нормативные предписания должны предусматривать минимальные компенсации, сглаживающие данный нестабильный характер занятости. Полагаем, что это должны быть положения об оплате минимума часов в любом случае, независимо от факта привлечения работника к работе (по примеру законодательства ФРГ, Нидерландов) [2], а также нормы, предусматривающие компенсацию ограничения прав работников в период ожидания (например, размер такой компенсации может варьироваться от характеристик накладываемых на работника ограничений).

Список литературы

1. Киселев И. Я. Личность в буржуазном трудовом праве. М.: Наука, 1982. 192 с.
2. Мотина Е. В. «Договор ноль часов» в зарубежном трудовом праве: понятие, причины, последствия // Трудовое и социальное право. 2023. № 2. С. 26-31.
3. Уборщиков улиц в Китае заставили носить умные браслеты. URL: https://dailymail.co.uk
4. Atkinson J. Zero-hours contracts and english employment law: Developments and possibilities. URL: https://journals.sagepub.com
5. Degryse Chr. Digitalisation of the economyand its impact on labour markets. URL: https://journals.sagepub.com
6. How hard will the robots make us work? URL: https://www.theverge.com
7. Jaehrling K., Kalina Th. Grey zones' within dependent employment: formal and informal forms of on-call work in Germany. URL: https://journals.sagepub.com
8. The Rise of Workplace Spying. URL: http://theweek.com
9. Thompson P., Van den Broek D. Managerial control and workplace regimes: an introduction. URL: https://journals.sagepub.com
10. Wood A. Powerful times: flexible discipline and schedule gifts at work // Work, Employment and Society. 2021. Vol. 32, № 6. Pp. 1061-1077.

Д. А. Новиков,
кандидат юридических наук, доцент,
Санкт-Петербургский государственный университет

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ПРИ НАЙМЕ РАБОТНИКОВ: ПРАВОВЫЕ ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ

Аннотация. Анализируются правовые проблемы использования технологий ИИ при найме работников, и обозначаются основные направления их решения. Автором выявлено, что решения, которые принимаются ИИ при найме работников, могут быть дискриминационными, создавать предпосылки для необоснованных отказов в приеме на работу. Обосновано, что защита трудовых прав в контексте

использования ИИ при найме работников требует кодирования ИИ в соответствии с локальными нормативными актами работодателя; письменного информирования потенциального работника об инструментах ИИ, которые используются для найма. Обозначается, что все решения, принятые ИИ, должны быть контролируемы и объяснимы работодателем, который и несет юридическую ответственность за их последствия. Выделяется понятие «предвзятый алгоритм». Констатируется, что для ИИ должен создаваться справедливый интерфейс, в который подаются данные, относящиеся конкретно к рассматриваемой вакансии, и который не содержит предвзятых алгоритмов. Решение данной проблемы видится в механизмах стандартизации и обязательной сертификация программного обеспечения, в котором задействована технология ИИ для найма работников.

Ключевые слова: искусственный интеллект, предвзятый алгоритм, работник, работодатель, наем на работу, дискриминация, необоснованный отказ, правосубъектность, юридическая ответственность

USING ARTIFICIAL INTELLIGENCE IN HIRING EMPLOYEES: LEGAL PROBLEMS AND PERSPECTIVES

Abstract. The article analyses the legal problems of using AI technologies in hiring employees and outlines the main directions of their solution. The author reveals that the decisions made by AI in hiring employees may be discriminatory and create prerequisites for unjustified refusals to hire. It is substantiated that the protection of labour rights in the context of the use of AI in hiring employees requires coding of AI in accordance with the local acts of the employer; written information of the potential employee about the AI tools used for hiring. It is stated that all decisions made by AI should be controlled and explained by the employer, who is legally responsible for their consequences. The author highlights the concept of "biased algorithm". The author states that a fair interface should be created for the AI, which is fed with data related specifically to the vacancy in question and does not contain biased algorithms. The author sees the solution to this problem in standardization mechanisms and mandatory certification of software that uses AI technology to hire employees.

Keywords: artificial intelligence, biased algorithm, employee, employer, hiring, discrimination, unreasonable refusal, legal personality, liability

Введение. Государственная политика в области развития цифровой экономики, базовые положения которой отражены в Паспорте национальной программы «Цифровая экономика Российской Федерации» (утв. протоколом Президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам от 04.06.2019 № 7), указывает на усиление процессов цифровизации в сфере занятости населения и отмечает необходимость одобрения концепции комплексного правового регулирования отношений, возникающих в связи с развитием цифровой экономики. В 2020 году авторы такой Концепции указали, что для трансформации законодательства в сфере цифровой экономики является необходимо сосредоточиться на изменениях трудового законодательства

в вопросах, которые касаются правовой защиты граждан в «условиях информационных технологических новаций в сфере труда и дистанционной занятости» [1]. Действительно, с учетом развития искусственного интеллекта (далее – ИИ) в Российской Федерации (например, Сбербанком уже запущен GigaChat – первый российский аналог ChatGPT4) программный интерфейс в сфере занятости не только в рамках государственных платформ, но и работодательских разработок непременно будет усложняться, что может произвести революцию в том, как работодатели нанимают работников, а также сформирует правовые риски, которые отметили авторы Концепции.

Поэтому основная правовая проблематика в данной сфере заключается в том, как следует регулировать технологии ИИ для сбора данных о людях в целях найма работников и как с юридической точки зрения оценивать их решения. Ведь ИИ изменил способ сбора и обработки данных о потенциальных работниках, собирая и используя большие объемы данных, что ранее было невозможно. А это, в свою очередь, создает дополнительные риски нарушения трудовых прав граждан в форме дискриминации и необоснованного отказа в приеме на работу. В результате перед работниками, работодателями, разработчиками и контролирующими органами встанет логичный вопрос о юридической ответственности за применение ИИ при найме работников и ее субъектах.

Проблематика использования ИИ при найме работников уже начала обсуждаться в российской [2, 3] и зарубежной юридической науке [4–7]. Однако на сегодняшний день большинство исследований являются фрагментарными, охватывающими отдельные участки данной научной проблемы. Вследствие этого следует обратить более пристальное внимание на правовые проблемы использования ИИ при найме работников и попробовать выработать универсальные рекомендации для их нормативного урегулирования.

Основная часть. За последние годы для сферы занятости в России было создано несколько государственных информационных систем: Единая цифровая платформа в сфере занятости и трудовых отношений «Работа в России», «Справочник профессий», Общероссийская социальная сеть деловых контактов Skillsnet, «Онлайнинспекция.рф». Исключительный прогресс среди данных систем показала платформа «Работа в России», изначально сформированная в качестве государственной информационной базы вакансий.

На сегодняшний день платформа «Работа в России» используется для поиска подходящей работы, для осуществления электронного кадрового документооборота в трудовых отношениях, а также для самостоятельного поиска работы и работников. Для осуществления последней функции на платформе «Работа в России» представлены специальные поисковые фильтры: регион, заработная плата, опыт работы, образование, график работы, тип занятости, тип вакансии, сфера деятельности и т. д. По данным фильтрам граждане, ищущие работу, и работодателя могут осуществлять отбор предложенных вакансий и опубликованных резюме. В этот технологический процесс задействован несложный, но все же ИИ, который позволяет отыскивать информацию и ранжировать ее по указанным в фильтрах приоритетам.

Работодателям разработчики предлагают следующие программные инструменты ИИ для найма работников:

– Paradox (год разработки программы: 2017; место разработки: Скоттсдейл, США). В алгоритм Paradox встроен виртуальный помощник Оливия, по сути являющий ботом по вопросам автоматизированного найма работников. В функционал Оливии входит сбор информации о потенциальных работниках, планирование и оценка собеседования. Клиенты Paradox – Unilever, Nestle и 3M;

– Sever.AI (год разработки программы: 2019; место разработки: Москва, Россия). Sever.AI позволяет осуществлять оценку резюме кандидатов, коммуникацию с помощью телефонной связи, электронной почты и чат-бота, проводить видеоинтервью, оценку которому дает и представитель работодателя, и ИИ. Последний анализирует видео по изображению (внешнему поведению), звуку речи (тембру голоса) и тексту (содержательности ответов). Sever.AI имеет базу кандидатов с фильтрами и тегами с двенадцати сайтов для поиска работы (например, HeadHunter, SuperJob, «Авито Работа»), которые аналогичным образом анализирует ИИ и предлагает работодателям для найма подходящих кандидатов. Технология ИИ Sever.AI используется в многофункциональном программном обеспечении для поиска работников «Поток Рекрутмент». Клиенты Sever.AI – «Северсталь», «Свеза», DNS, «ДодоПицца»;

– VCV (год разработки программы: 2010; место разработки: Москва, Россия). VCV осуществляет отбор резюме кандидатов, организацию звонков и запись видеоинтервью с распознаванием ИИ лица и голоса. VCV позволяет просматривать видеоролики, а к моменту личной встречи исключить заведомо неподходящих кандидатов, предварительно оценить soft skills и соответствия ценностям компании для оценки настроения и поведения кандидатов. Клиенты VCV – «Билайн», «Сибур», Danone, Mars, Citibank.

Кроме указанных ИИ-инструментов найма работников, в России используются Playhunt, HireVue, uForce, Hireman, PeopleForce, AmazingHiring, Recright, FriendWork Recruiter, Hurma, Talantix, СберПодбор, «Робот Вера», GoRecruit и др. В зарубежных странах распространены такие платформы, как AllyO, TextRecruit, Zoom.ai, Textio, Ideal, Jibe, Taleo, Arya, Entelo, BambooHR и ZohoRecruit. Следует учесть, что данные сервисы ИИ для найма работников перманентно усовершенствуются, дополняются новыми функциями, в том числе благодаря технологии машинного обучения.

Машинное обучение включает в себя алгоритмы, которые обучаются на основе данных, основанных на прошлом поведении и практике человека, и которые затем разрабатываются для использования в будущем. Машинное обучение являет собой инструмент обучения и развития ИИ, когда тот подвергается воздействию данных и закономерностей, которые система выявляет после выполнения различных задач и воспроизводит данный процесс до того момента, пока не получает достаточно данных.

Это означает, что с помощью алгоритмов машинного обучения, закодированных в ИИ, могут быть найдены закономерности или предпочтения, которые не воспринимались другими людьми, включая самого субъекта данных, что в свою

очередь создает почву для дискриминации при найме работников и может повысить риски необоснованных отказов в приеме на работу. Например, в результате такой практики могут возникнуть проблемы, особенно когда работодатели могут запрограммировать систему ИИ не нанимать конкретного человека на одну должность, а впоследствии система узнает, что этот человек не подходит ни для какой другой должности. Необходимо заметить, что система ИИ, созданная для подбора работников, может сделать это только в том случае, если она была запрограммирована и обучена определенным образом, а также с использованием исторических данных о найме.

Технология ИИ обладает потенциалом для сбора данных о потенциальных работниках и их обработки в интересах работодателя при найме кандидатов на конкретную должность. По своим технологическим возможностям ИИ может генерировать подробную информацию, касающуюся частных данных, найденных в открытых профилях социальных сетей, и предоставлять подробные отзывы и биографические данные о потенциальных работниках для целей найма. Идея использования технологий ИИ заключается в том, что в базу данных работодателя может быть загружено большое количество резюме, а ИИ может быстро обработать эти заявки и направить работодателю лучших кандидатов.

То есть, используя ИИ, данные сайтов с резюме (например, информацию из платформ «Работа в России», HeadHunter, SuperJob, «Авито Работа» и др.), социальные сети (например, открытых данных из профиля «ВК» или «Одноклассники») и машинное обучение, работодатели имеют более широкий доступ к частной жизни и личным качествам кандидатов. Машинное обучение обладает потенциалом для измерения и обработки определенных характеристик из профилей социальных сетей. Полагаясь на такие данные, можно создать риск формирования потенциального неравенства при найме, что уже было подтверждено случаем в компании Amazon. Технология ИИ компании Amazon была признана дискриминационной, поскольку она сама себя научила тому, что кандидаты-мужчины предпочтительнее кандидатов-женщин, и осуществляла соответствующий подбор претендентов на открытие вакансии. Программа нашла выражения, используемые мужчинами в резюме (а именно слова «исполнять» и «заканчивать»), более убедительными. ИИ решил, что самопрезентация мужчинами своих трудовых достижений была более эффективной. Кроме того, система обучалась на резюме, представленных претендентами, получившими работу за десятилетний период, большая часть из которых поступила от мужчин [8]. То есть в зависимости от того, как настроены системы ИИ, они могут дискриминировать людей и отсеивать тех, кто им не нравится, или ранжировать резюме людей на основе несправедливых критериев, выработанных машинным обучением. Потенциальный эффект заключается в том, что система ИИ при фильтрации данных различает «безопасных» людей и тех, кого следует избегать, и может отнести кандидатов к определенным категориям, например, к «хорошим» или «плохим» работникам.

Работодатели, применяя данные технологии предполагают, что инструменты ИИ объективны и поэтому могут управлять процессом принятия решений, свободным от предвзятости, которая влияет на человеческие суждения [8]. И со-

ответственно логичным может показаться вывод, что риск дискриминации и необоснованного отказа в приеме на работу при использовании ИИ уменьшается, как и риск найма на работу менее квалифицированного работника. Однако такое предположение подразумевает, что разработчики этих алгоритмов, данные, на которых строятся эти инструменты, и организации, в которых они применяются, беспристрастны.

Поскольку инструменты ИИ управляются данными, полученными из человеческого общества, трудно, если не невозможно избежать риска того, что инструменты ИИ закодируют и усугубят существующие предубеждения [9]. В некоторых отношениях любая предвзятость в процессах принятия решений, управляемых ИИ, может быть смягчена способами, которые обычно невозможны при человеческом суждении. Человеческое решение обычно не фиксирует все различные исходные данные и процессы рассуждения, которые входят в это решение (на самом деле люди могут даже не осознавать все исходные данные, которые вошли в конечное решение). Но алгоритмические процессы принятия решений по своей сути зависят от того, насколько формальными и явными являются любые критерии принятия решений, что создает возможность для обнаружения и устранения источников предвзятости. Соответственно, такой алгоритм можно условно назвать предвзятым.

Чтобы обнаружить (и, возможно, изменить) предвзятый алгоритм, сначала необходимо определить, что такое предвзятый алгоритм. Предвзятый алгоритм – это алгоритм, который несправедливо приводит к различным результатам для людей из разных социальных групп. Как отмечает Ю. С. Харитонова, «алгоритмическая предвзятость наличествует даже в тех случаях, когда у разработчика алгоритма отсутствуют намерения осуществлять дискриминацию, и даже в случаях непринятия на вход демографической информации, рекомендуемой системой» [10]. То есть предвзятый алгоритм представляет собой алгоритм, приводящий к дискриминации, необъективным и незаконным решениям. При этом ввиду указанных особенностей машинного обучения возможна лишь минимизация риска предвзятости алгоритмов с помощью технических и юридических механизмов.

Недискриминационным при найме работника, считается такой результат, при котором работодатель выбирает кандидата с наилучшим сочетанием квалификации и деловых качеств, соответствующих данной должности. В соответствии со ст. 195.1 Трудового кодекса РФ квалификация работника – это уровень знаний, умений, профессиональных навыков и опыта работы работника. В п. 10 Постановления Пленума Верховного Суда РФ от 17.03.2004 №2 «О применении судами Российской Федерации Трудового кодекса Российской Федерации», при определении понятия деловых качеств используется словосочетание «в частности». Это указывает на то, что признаки деловых качества не имеют исчерпывающего характера. То есть законодательство не ограничивает работодателя в приемах и способах проверки деловых качеств. Аналогичная позиция представлена в судебной практике по делам о проведении различного, в том числе психологического, тестирования при приеме на работу для проверки деловых качеств.

Таким образом, на сегодняшний день отсутствует юридическая регламентация процедуры оценивания деловых качеств работника. Поэтому работодатель может самостоятельно избрать форму, в которой он будет осуществлять такую оценку, и закрепить ее в локальных нормативных актах организации. Поэтому крайне важно кодировать точные данные в программах ИИ для найма работников, чтобы избежать дискриминации и необоснованного отказа в приеме на работу. Кроме того, недопущение дискриминации и необоснованного отказа в приеме на работу должно обеспечиваться письменным информированием потенциального работника об инструментах ИИ, которые использованы для анализа цифровой информации.

Нужно заметить, что, даже если ИИ будет запрограммирован с минимизацией риска предвзятых алгоритмов, открытым остается вопрос об ответственности за принятие решения о найме работника либо отказе в приеме на работу при использовании ИИ.

Признание юридической ответственности непосредственно ИИ за принятие решения о найме работника не выдерживает никакой критики, так как алгоритмы ИИ не являются и не могут являться субъектом права и не обладают правосубъектностью. Хотя в современных исследованиях существуют позиции, что прикладное управление ИИ уже стало способным сделать видимость того, будет ли программа посылать свои собственные решения работнику [11], или что нынешние информационно-социальные изменения затрагивают и трансформируют характер трудовых отношений в основном таким образом, что личное общение субъектов отношения отходит на второй план, а личное отношение будет заменено отношениями между работником и цифровой средой [12], но данные позиции не выдерживают критики. ИИ не может более быть участником общественных отношений, так как не имеет способности устанавливать взаимодействие между субъектами права по поводу удовлетворения материальных или культурных потребностей. Также не существует никакого общественно значимого результата, которого ИИ хотел бы достичь. Иных субъектов права ИИ может исключительно датифицировать под конкретные алгоритмические задачи, заданные при программировании и усовершенствованные путем машинного обучения. Поэтому признание за ИИ правосубъектности невозможно, исходя из программного свойства его взаимосвязи с внешним миром. ИИ в правовой реальности может существовать исключительно в качестве объекта права. ИИ является средством автоматизации процессов найма потенциальных работников, цифровым интерфейсом взаимодействия между элементами производственной системы на уровне сбора, анализа и обработки информации. Все решения, принятые ИИ при найме на работу и в рамках трудовых отношений, должны быть контролируемы и объяснимы работодателем, который и несет ответственность за их последствия.

Исходя из сложности технологии ИИ и машинного обучения, а также рисков использования работодателем программного обеспечения с наличием предвзятого алгоритма, для обеспечения защиты трудовых прав граждан от дискриминации и необоснованных отказов в приеме на работу и обеспечения информационной безопасности персональных данных, актуальным является стандартизация и сертификация программного обеспечения, в котором задействована технология ИИ.

Необходимо отметить, что в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. ИИ определяется как комплекс технологических решений. Согласно ФЗ от 29.06.2015 № 162-ФЗ «О стандартизации в Российской Федерации» и ФЗ от 27.12.2002 № 184-ФЗ «О техническом регулировании», ИИ может быть объектом стандартизации и сертификации.

Федеральное агентство по техническому регулированию и метрологии на период 2021–2024 гг. приняло Перспективную программу стандартизации по приоритетному направлению «Искусственный интеллект», которая предполагает создание 217 стандартов в сфере ИИ. К сожалению, в перечне данных стандартов отсутствуют стандарты в сфере использования ИИ для найма работников. Для разработки и внедрения стандарта в сфере использования ИИ для найма работников следует обратиться к уже принятому в 2020 г. базовому стандарту «Системы искусственного интеллекта. Способы обеспечения доверия. Общие положения» (ГОСТ Р 59276-2020). В этом документе определяется понятие «доверие к системам ИИ»; приводится классификация факторов, которые влияют на качество и способность систем ИИ вызывать доверие на стадиях жизненного цикла; формализуется взаимосвязь качества и способности систем ИИ вызывать доверие; указывается классификация основных способов обеспечения доверия к системам ИИ. Также нужно учесть положения ГОСТ Р 59277-2020б от 03.01.2021, которым утвержден «Национальный стандарт системы искусственного интеллекта. Классификация систем искусственного интеллекта». Данным государственным стандартом устанавливаются принципы классификации систем ИИ.

Сертификация программного обеспечения и алгоритмов ИИ на сегодняшний день не является в России обязательной согласно Постановлению Правительства РФ от 01.12.2009 № 982 «Об утверждении единого перечня продукции, подлежащей обязательной сертификации, и единого перечня продукции, подтверждение соответствия которой осуществляется в форме принятия декларации о соответствии». Программное обеспечение проходит подтверждение соответствия с заявленным производителем ТУ или ГОСТ исключительно в добровольной системе сертификации продукции. В свою очередь, развитие систем ИИ и возникновение существенных рисков, связанных с возможным нарушением трудовых прав граждан и их информационной безопасностью, требует включения в перечень продукции, подлежащей обязательной сертификации, программ ИИ и машинного обучения на основе разработанных государственных стандартов.

Заключение. Использование ИИ при найме работников формирует значительное количество правовых проблем. Решения, которые принимаются ИИ в процессе сбора, обработки и анализа данных о потенциальном работнике, могут быть дискриминационными, создавать предпосылки для необоснованных отказов в приеме на работу, нарушать право на неприкосновенность частной жизни.

Недопущение дискриминации и необоснованного отказа в приеме на работу должно обеспечиваться кодированием ИИ в соответствии с локальными нормативными актами работодателя, где содержится программа и методика тестирования, и должностной инструкции. Потенциальные работники также должны быть осведомлены о том, как собирается и обрабатывается их информация ИИ

для определения возможности их найма на конкретную вакансию. Кроме того, недопущение дискриминации и необоснованного отказа в приеме на работу должно обеспечиваться письменным информированием потенциального работника об инструментах ИИ, которые используются для анализа цифровой информации.

С юридической точки зрения ответственность за принятие решения о найме работника несет исключительно работодатель, так как ИИ не является субъектом права и не обладает правосубъектностью. ИИ в правовой реальности может существовать исключительно в качестве объекта права. Все решения, принятые ИИ, должны быть контролируемы и объяснимы работодателем, который и несет ответственность за их последствия. Окончательное решение о найме работника либо об отказе в приеме на работу на основе информации, полученной от ИИ, может принимать исключительно работодатель и его уполномоченный орган.

Для недопущения нарушения указанных прав граждан системы ИИ должны быть запрограммированы надлежащим и справедливым образом. Программисты систем ИИ должны создавать интерфейс, в который подаются данные, относящиеся конкретно к рассматриваемой вакансии, и который не содержит предвзятых алгоритмов. Для решения данной проблемы актуальными являются стандартизация и сертификация программного обеспечения, в котором задействована технология ИИ.

Список литературы

1. Концепция комплексного регулирования (правового регулирования) отношений, возникающих в связи с развитием цифровой экономики. М.: Ин-т законод. и сравн. правоведения при Правительстве Российской Федерации, 2020. 32 с.

2. Щербакова О. В. Использование программ искусственного интеллекта при найме работников // Электронное приложение к Российскому юридическому журналу. 2021. № 3. С. 72-76.

3. Serova A. V., Shcherbakova O. V. The Employee's Right to Privacy Transformation: Digitalization Challenges // Kutafin Law Review. 2022. № 9(3). P. 437-465.

4. De Stefano V. Negotiating the Algorithm: Automation, Artificial Intelligence, and Labor Protection // Comparative Labor Law & Policy Journal. 2019. 41(1). Pp. 15-46.

5. Reddy S. The Legal Issues Regarding the Use of Artificial Intelligence to Screen Social Media Profiles for the Hiring of Prospective Employees // Obiter. 2022. № 43 (2). Pp. 113-131.

6. Köchling A., Wehner M. C. Discriminated by an Algorithm: a Systematic Rreview of Discrimination and Fairness by Algorithmic Decision-making in the Context of HR Recruitment and HR Development // Business Research. 2020. № 13. Pp. 795-848.

7. Hunkenschroer A. L., Kriebitz, A. Is AI Recruiting (Un)ethical? A Human Rights Perspective on the Use of AI for Hiring // AI Ethics. 2023. № 3. Pp. 199-213.

8. Oppenheim M. Amazon Scraps "Sexist AI" Recruitment Tool. URL: https://www.independent.co.uk

9. Artificial Intelligence: Examples of Ethical Dilemmas. URL: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics/cases

10. Харитонова Ю. С., Савина В. С., Паньини Ф. Предвзятость алгоритмов искусственного интеллекта: вопросы этики и права // Вестник Пермского университета. Юридические науки. 2021. Вып. 53. С. 488-515.

11. Ivanova M., Bronowicka J., Kocher E., Degner A. The App as a Boss? Control and Autonomy in Application-Based Management. Working Paper Forschungsförderung. 2018.

12. Lőrincz, G. Kommentár a munka törvénykönyvéről szóló 2032. évi I. törvényhez: Munkajogi sci-fi // Pécsi Munkajogi Közlemények. 2018. № 11(1-2). Ol. 7-34.

С. М. Новрадова-Василиади,
кандидат юридических наук, доцент,
Академия труда и социальных отношений

ТЕНДЕНЦИИ ЦИФРОВИЗАЦИИ ТРУДОВОГО ПРАВА В РОССИЙСКОЙ ФЕДЕРАЦИИ И ОТДЕЛЬНЫХ СТРАНАХ ЕВРОПЕЙСКОГО СОЮЗА

Аннотация. В статье уделено внимание направлениям формирования тенденций цифровизации трудового права как в Российской Федерации, так и в отдельных странах Европейского союза. Выделяются вопросы правового регулирования рабочего времени дистанционных работников и предпосылки формирования трансформационных процессов в отрасли трудового права. Отдельно рассмотрены вопросы правовых механизмов минимизации последствий цифровизации в некоторых странах Европейского союза.

Ключевые слова: труд, цифровые технологии, рабочее время, работник, дистанционный труд, цифровизация, работодатель

TRENDS IN DIGITALIZATION OF LABOR LEGISLATION IN THE RUSSIAN FEDERATION AND IN CERTAIN COUNTRIES OF THE EUROPEAN UNION

Abstract. The author draws attention to the directions of trend formation in the digitalization of labor law both in the Russian Federation and in individual countries of the European Union. The issues of legal regulation of working hours of remote workers and conditions for the formation of transformational processes in the field of labor law are highlighted. The issues of legal mechanisms for minimizing the consequences of digitization for individual countries of the European Union are considered separately.

Keywords: labor, digital technologies, working time, employee, remote work, digitalization, employer

Внедрение новых форм коммуникаций между людьми, создание новых технологий, которые приводят к формированию в обществе новых понятий и право-

вых конструкций и механизмов являются двигателем трансформационных процессов в современном обществе, которые обуславливают стремительное развитие цифровых технологий, затрагивающее все сферы общества и изменяющее структуру экономики [3].

Современная культура, созданная такими цифровыми технологиями как компьютер и Интернет, сформировала дефицит ориентации в рамках получения самой информации, используя данные цифровые инструменты. То есть дефицит количества времени, для того чтобы выделить время избыточно прибывающей информации. Управление знаниями – одна из главных задач современного общества в культуре использования цифровых технологий, которое должно сосредоточиться, прежде всего, на фильтрации релевантной, имеющей прямое отношение к задаче информации для принятия решений в условиях неопределенности и недостатка времени. Непрерывное получение, отправление и сохранение информации и определяет тот факт, что мы включены в мировую коммуникацию [5].

В последние годы, по мнению экспертов в области трудового права наблюдается тенденция к сокращению рабочих мест в условиях цифровизации в отдельных сферах экономики. В этой связи посредством глобального, регионального и национального государственно-частного сотрудничества принимаются все необходимые меры для адаптации работников в новых условиях труда и их трудоустройства [3].

Ведение коллективных переговоров как один из адаптационных инструментов является основополагающим инструментом, позволяющим обеспечить и защитить трудовые права работников на рынке труда [7–8].

В результате коллективных переговоров в отдельных странах Европейского союза, например, в Германии, заключаются тарифные договоры о цифровизации с работниками. Такие договоры предусматривают правовые и экономические меры по поддержке работников, чей труд подвержен изменениям в условиях цифровизации, а именно изменению рабочих процессов, метода работы, машин и оборудования, изменению организации труда и т. д. [3].

В Российской Федерации изменения в трудовом праве и его отдельных институтах в настоящее время в новых условиях во многом предопределены также развитием цифровых технологией – цифровизацией трудового права [4].

Явным примером являются изменения, происходящие в правовом регулировании рабочего времени работников при дистанционном режиме труда. Часть 1 ст. 312.4 Трудового кодекса РФ регламентирует режим работы и отдыха дистанционных работников. Очевидно, что возникают определенные проблемы при разработке режима труда рабочего времени дистанционному работнику. В соответствии с указанной статьей режим рабочего времени и времени отдыха дистанционного работника устанавливается им по своему усмотрению, если иное не предусмотрено трудовым договором, дополнительным соглашением к трудовому договору, коллективным договором, локальным нормативным актом. Это не освобождает работодателя от обязанности вести учет рабочего времени такого работника. Причем время взаимодействия дистанционного работника с работодателем включается в рабочее время.

Установленный самостоятельный выбор работника может привести к возникновению определенных рисков. Во-первых, сложность контроля рабочего времени при дистанционном режиме труда. Во-вторых, проблемы взаимодействия для оперативного решения вопросов. Доступность работника в рабочее время может не совпадать с режимом труда остальных сотрудников, взаимодействие которых необходимо для оперативного решения задач. Поэтому следует определять границы дистанционного времени работы.

В-третьих, выполнение работником своих трудовых обязанностей в ночное время, в выходные дни, праздники или за переделами нормы рабочего времени, установленной законом, оплачиваются в повышенном размере. Возможны злоупотребления и потенциальные споры в части оплаты труда в повышенном размере.

График работы сотрудника при дистанционной работе регламентируется правилами внутреннего трудового распорядка. Как правило, в них устанавливается общий режим для всех сотрудников. В соответствии со ст. 190 Трудового кодекса правила внутреннего трудового распорядка разрабатываются и утверждаются с участием коллектива (порядок согласования с представительным органом работников указан в ст. 372 ТК РФ). Все новые работники (в том числе дистанционные) знакомятся с документом до подписания трудового договора. Однако существуют случаи на практике, когда режим работы конкретного сотрудника отличается от принятого в организации и установленного в правилах внутреннего трудового распорядка. В таких случаях в соответствии со ст. 57 ТК РФ положение по дистанционному режиму работы включается непосредственно в трудовой договор.

Применение суммированного учета рабочего времени в отношении дистанционных работников на практике встречается редко. Для защиты интересов работодателя рекомендуется применять учет по дням. Но здесь существуют определенные сложности, так как у работодателя зачастую нет инструментов и механизмов контроля о начале и окончании работником своих трудовых обязанностей. В этой связи механизм контроля выполнения трудовых обязанностей необходимо закреплять в трудовом договоре и локальном нормативном акте. Что касается документов учета рабочего времени, то законодатель отводит этот вопрос на усмотрение работодателей. По общему правилу учет режима работы дистанционного работника ведется в унифицированной форме. Но работодатель может ввести свою форму такого учета.

Особое внимание следует уделить изучению и анализу судебных актов о привлечении к административной ответственности дистанционных работников. Проанализировав судебную практику, можно сделать вывод о том, что существуют спорные вопросы привлечения к дисциплинарной ответственности дистанционных работников.

Как видно из практики, суды не всегда признают увольнение работника по пп. а, п. 6 ст. 81 ТК РФ (т. е. прогул, отсутствие на рабочем месте без уважительных причин в течение всего рабочего дня (смены), независимо от его (ее) продолжительности, а также в случае отсутствия на рабочем месте без уважительных причин более четырех часов подряд в течение рабочего дня (смены)) законным если работник не был на рабочем месте, т. е. за прогул, а такие факты, как непре-

доставление еженедельных отчетов в электронном виде, то, что работник не отвечал на звонки и не перезвонил недостаточны для увольнения работника [1].

Тем временем апелляционным определением Санкт-Петербургского городского суда установлено, что между сторонами спора был заключен трудовой договор о дистанционной работе, основанием для привлечения работника к дисциплинарной ответственности явились докладная записка, акт о невыполнении условий трудового договора, согласно которым дистанционный работник прекратил вести оперативную служебную переписку и прервал деловое взаимодействие с руководителем, не подтвердил получение запроса и не представил отчета о выполнении задачи. Суд признал, что выявленные нарушения неисполнения трудовых обязанностей имели место, факт совершения работником дисциплинарного проступка, повлекшего наложение дисциплинарного взыскания, подтвержден, процедура применения взыскания работодателем нарушена не была [2]. Суд, оценивая доводы работника о том, что у него отсутствовала техническая возможность исполнить задания работодателя, поскольку директором по продажам у него был изъят рабочий компьютер, суд, между тем, обратил внимание на то, что трудовой договор о дистанционной работе, заключенный между сторонами, не содержит обязанности работодателя обеспечить работника рабочим компьютером.

В современных условиях цифровизация труда имеет свои достоинства и недостатки для сторон трудовых отношений, однако в России рассматривается как положительный процесс, несмотря на трудности, которые сталкиваются при внедрении на практике и правовом регулировании.

Список литературы

1. Апелляционное определение СК по гражданским делам Волгоградского областного суда от 23 марта 2018 г. по делу № 33-3223/2018 // СПС «КонсультантПлюс».

2. Апелляционное определение Санкт-Петербургского городского суда от 16.09.2019 № 33-19910/2019 по делу № 2-896/2019 // СПС «КонсультантПлюс».

3. Избиенова Т. А., Вайман А. Б. Коллективный (тарифнй) договор в эпоху цифровизации в Германии // Кадровик. 2023. № 5. С. 56-60.

4. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7-32. EDN LCCOJJ

5. Хойна М. Н. Рынок труда в условиях цифровой трансформации экономики. URL: https://elar.urfu.ru/bitstream/10995/103624/1/978-5-8295-0768-8_2021_70.pdf?ysclid=l0unr4bb5u

6. Цифровая трансформация отраслей: стартовые условия и приоритеты: докл. к XXII Апр. междунар. науч. конф. по проблемам развития экономики и общества. Москва, 13–30 апр. 2021 г. / Г. И. Абдрахманова, К. Б. Быховский, Н. Н. Веселитская, К. О. Вишневский, Л. М. Гохберг и др. ; рук. авт. кол. П. Б. Рудник; науч. ред. Л. М. Гохберг, П. Б. Рудник, К. О. Вишневский, Т. С. Зинина; Нац. исслед. ун-т «Высшая школа экономики». М.: Изд. дом Высшей школы экономики, 2021. 239 с.

7. De Stefano V. Algorithmic management and collective bargaining // Artificial Intelligence, Platform Work and Labor. URL: http: ssrn.com/abstract=4139319

8. De Stefano V. Non -Standart work and limits on freedom of Association: A Human Rights Based Approach // Industrial Law Journal Advance Access published. URL: https://www.bollettinoadapt.it/wp-content/uploads/2016/10/Ind-Law-J-2016-De-Stefano.pdf

С. В. Парамонова,
старший преподаватель,
Уральский государственный юридический университет
имени В. Ф. Яковлева

МЕТАМОРФОЗЫ РАБОТЫ ПО ВЫЗОВУ В ЦИФРОВУЮ ЭПОХУ

Аннотация. Работа по вызову относится к числу давно известных, но неравномерно и неоднообразно применяемых, поэтому фрагментарно исследованных практик организации труда. В России к работе по вызову скептическое отношение. Опасения по поводу прекаризации труда вынуждают отвергать такой вариант работы, а неудачи в опыте других стран блокируют поиск решений, которые в условиях национального правопорядка могли бы стать успешными. Вместе с тем цифровая эпоха настойчиво подталкивает к гармоничному сочетанию различных форм занятости на рынке труда и эволюции классических трудовых отношений согласно потребностям общества и государства. Работа по вызову – зона средних прекаризационных рисков, снижать которые можно через повышение уровня определенности, что исключает заимствование зарубежной практики без осмысления природы явления. Работа по вызову – нечто большее, чем просто нестандартная форма занятости, поэтому у нее гораздо больше шансов занять свою нишу при конкуренции с другими схожими способами организации труда.

Ключевые слова: Нестандартные формы занятости, работа по вызову, гибкое рабочее время, разовая работа, время нахождения в состоянии готовности, дежурство, прекаризация

METAMORPHOSES OF CALL WORK IN THE DIGITAL AGE

Abstract. On-call work is one of the long-known, but unevenly and heterogeneously applied, therefore, fragmentary researched practices of labor organization. In Russia, there is a skeptical attitude towards work on call. Concerns about the precarization of labor force this option to be rejected, and failures in the experience of other countries block the search for solutions that, under the conditions of the national legal order, could become successful. At the same time, the digital age is persistently pushing for a harmonious combination of various forms of employment in the labor market and the evolution of classical labor relations in accordance with the needs of society and the state. On-call work is a zone of medium precarious risks, which can be reduced by increasing the level of certainty, which excludes the borrowing of foreign practice

without understanding the nature of the phenomenon. Call work is more than just a non-standard form of employment, so it is much more likely to find its niche when competing with other similar ways of organizing work.

Keywords: non-standard forms of employment, on-call work, flexible working hours, casual work, time spent in a state of readiness, duty, precarization

Международная организация труда (далее – МОТ) в докладе «Мировая занятость и социальные перспективы: тенденции 2023 г.», опубликованном в самом начале года [14], в очередной раз акцентирует внимание, что достойный труд, т. е. труд, который обеспечивает достаточный заработок, безопасность на рабочем месте и социальную защиту, – основной ориентир национальных политик и регулирования. МОТ считает, что технологический прогресс пока не в полной мере оправдал оптимистические прогнозы, в частности по росту производительности труда. Сегодня не происходит таких технологических прорывов, которые могли бы принести пользу обществу, облегчали бы, например, переход к удаленной работе или гибридной форме трудовой деятельности или удовлетворяли потребности в инновационных решениях в интересах сотрудничества на все более многообразном рынке труда.

Активизировать технологическое развитие в областях, имеющих особую социальную значимость, МОТ полагает возможным за счет инновационных методов нормативно-регуляторной деятельности с использованием комплексного подхода в нормотворчестве и государственных закупках, а также тесного взаимодействия между социальными партнерами в целях повышения производительности. МОТ констатирует, что в мире сложилась обстановка постоянной и высокой неопределенности, которая вредит инвестициям в бизнес, обесценивает реальную заработную плату, вынуждает работников возвращаться к неформальным трудовым отношениям. По данным МОТ, в 2022 году в мире насчитывалось около 2 млрд работников, занятых неформально, а значит, лишенных социальной защиты.

В условиях турбулентности, к которой мир, кажется, начинает не только привыкать, но и приспосабливаться, неопределенность свойственна не только будущему, но и прошлому. Все труднее понять причинно-следственные связи и истинную природу вещей и явлений. Крайне подвижна семантика слов, а за ними терминов, понятий, категорий. Понятийный аппарат и законы естественных наук помогают экспертам точнее объяснить реальность, но чем понятнее реальность, тем больше опасений (в силу неочевидности связей между влиянием и его последствиями) вызывает «эффект бабочки» Э. Лоренца. В прошлом видится многообразие и запутанность причинно-следственных связей, взгляд в будущее уже менее решителен.

В этом контексте любопытны метаморфозы, которые происходят в области нестандартной организации труда. Так, работа по вызову с большой долей вероятности заставит современного человека хотя бы на секунду, но задуматься над вопросом, о чем конкретно идет речь, а размышления с учетом места его проживания, возраста, профессии, опыта и т. д. наверняка приведут к разным результатам. Вполне может оказаться, что к работе по вызову можно отнести сверхурочную

работу, работу в выходной день, отзыв из отпуска, дежурство. Кто-то однозначно свяжет работу по вызову и платформенную занятость, а кто-то будет убежден, что научно-технический прогресс обусловил появление такой работы. Несмотря на то, что к новации работу по вызову отнести нельзя, многим правопорядкам она до сих пор неизвестна.

Работа по вызову считается нестандартной и неустойчивой занятостью, для которой характерна гибкость рабочего времени. Тенденция развития гибких режимов рабочего времени начала проявляться в конце XX века и в свете зарождающейся концепции work-life balance изначально рассматривалась в позитивном ключе. Опираясь на мнение западных коллег, И. Я. Киселев писал, что модернизированная организация труда будет иметь далеко идущие последствия и в XXI веке для использования рабочей силы будет характерен учет специфики личности (возраст, семейное положение, психика, личные наклонности, жизненный биологический ритм). Он отмечал, что легализация мобильных режимов, в том числе работы по вызову, происходила за рубежом в несколько этапов: сначала на уровне трудовых договоров, затем на уровне правил внутреннего трудового распорядка и коллективных договоров, наконец, в некоторых странах соответствующие положения нашли свое закрепление на уровне законодательства [7. С. 114–116].

После того как не только в развивающихся, но и развитых странах значительно увеличилась доля временной работы, работы с неполным рабочим временем, чрезмерная гибкость и индивидуализм стали вызывать озабоченность. В структуре общества ученые выделили особый социальный слой – прекариат (люди, не имеющие полной гарантированной занятости). Исследуя проблемы наемного труда, французский социолог Р. Кастель пришел к выводу, что рост безработицы, нестабильная занятость, атипичные формы занятости, проявившие себя в последние два десятилетия XX века, являются закономерным результатом кризисов [6. С. 462–463]. Британский экономист Г. Стэндинг, призывая осознать мировую проблему формирования из «лишних людей» нового класса («лишние люди» – термин Р. Кастеля, результат «кризиса» и «деконверсии»), главной непосредственной причиной роста прекариата назвал переход к гибким трудовым отношениям [20. С. 61].

Г. Стэндинг выделяет три направления гибкости в сфере труда: гибкость численности, гибкость функциональности и гибкость заработной платы. Работа с нулевым рабочим временем, частичная и временная занятость являются способами управления численностью [20. С. 62–69]. С точки зрения экономики гибкость обеспечивает снижение затрат, а значит, увеличение прибыли. Снижать затраты требуется при кризисе, а также для того, чтобы обеспечить рост и развитие. Сравнивая достоинства и недостатки традиционной модели трудовых отношений для работника, работодателя и государства с применением категорий «риск» и «издержки», российские экономисты полагают, что ее сохранение в условиях постиндустриальной экономики возможно только в том случае, если для всех заинтересованных сторон ее достоинства перевесят ее недостатки [2. С. 182].

Прекаризация, усиливающаяся под воздействием цифровых технологий, социологами и экономистами изучается в контексте трансформации сферы труда,

при которой становятся еще более уязвимы социальные и экономические позиции групп и отдельных индивидов. В поле зрения находятся такие ее проявления, которые связаны с потерей средств к существованию и разрывом социальных связей, неполноценностью гражданского статуса. Исследователями утверждается, что феномен цифровизации труда и занятости является фактором социального загрязнения от экономической деятельности хозяйствующих субъектов [21. С. 31]. Между тем прекаризацию можно определить как процесс или состояние, результатом или характеристикой которых является отсутствие определенности в той степени, которая достаточна для обеспечения безопасности, исключения неблагоприятных последствий.

В связи с этим справедливы следующие выводы, к которым приходят отдельные исследователи: 1) феномен прекаризации не ограничивается вопросами трудовых отношений, а формирует явление общей жизненной нестабильности; 2) стандартные рабочие места также подвержены рискам прекаризации, в то время как далеко не все нестандартные приводят к уязвимости положения работников [18. С. 110]. Тем не менее отрицательное отношение к феномену прекаризации пока превалирует, поэтому применение соответствующей терминологии в большинстве случаев более чем аккуратное. В российских правовых исследованиях подобные термины встречаются редко и зачастую в узких предметных областях, попытки обобщения единичны [11. 25, 27].

Разделяя позицию о том, что в терминах «нестандартные формы занятости», «нетипичные формы занятости», «атипичные формы занятости», «гибкие формы занятости» имеется неопределенность, которая «не способствует делу научного познания и не обеспечивает юридико-технические требования, предъявляемые к правотворческому процессу» [28. С. 213–214], следует отметить, что в обзоре МОТ, на который все обращают внимание, акцент, по сути, сделан на факторах распространения нестандартных форм занятости и на прекаризационных рисках. В обзоре «Нестандартные формы занятости. Анализ проблем и перспективы решения в разных странах» (обзорная версия отчета, 2017 г.) [15] МОТ указывает, что «нестандартные формы занятости» – собирательный, другими словами, как отмечают в публикациях, «зонтичный» термин [10. С. 57].

Работа по вызову включена МОТ в перечень нестандартных форм занятости. Данные формы демонстрируют дефицит качественных условий труда по направлениям: трудоустройство, заработок, график работы, безопасность и гигиена труда, социальное обеспечение, обучение, представление интересов и другие основополагающие принципы и права. При этом МОТ отмечает, что дефициты качественных условий труда по этим направлениям могут присутствовать в стандартных трудовых отношениях [15. С. 16]. Получается, что классическая занятость является зоной минимальных прекаризационных рисков, а нестандартные формы занятости с отклонениями по сроку трудового договора, рабочему времени, прямому подчинению конечному пользователю, а также занятость вне рамок трудовых отношений – это зона повышенных прекаризационных рисков.

В одном из исследований посредством оценки нестандартных форм занятости на соответствие признакам достойного труда, перечисленным в одноименной

программе МОТ 1999 г., показано, за счет чего усиливаются прекаризационные риски при нестандартной занятости [13. С. 109–110]. Имеет смысл согласиться с авторами, что идентификация прекаризационных рисков позволяет разрабатывать мероприятия по их снижению. В развитие этой идеи с целью системной разработки мероприятий предлагается 4 укрупненные группы нестандартных форм занятости, содержащие в себе подгруппы в зависимости от национальной специфики, которые определены МОТ, ранжировать по категориям прекаризационных рисков (умеренный, средний, значительный и высокий). Видится, что работа по вызову все-таки подразумевает средние прекаризационные риски.

Развитие под воздействием современных технологий гиг-экономики (экономики по требованию) предопределено тем, что она при минимуме издержек удовлетворяет запрос на скорость, многообразие выбора и результат, более органичен ее контакт с концепцией work-life balance. Работа по вызову в свое время была призвана закрывать аналогичные потребности, в ней заложен тот же ключевой принцип использования труда только тогда, когда в этом имеется необходимость. На фоне гонки за снижением издержек дифракционная тенденция, т. е. перерождение работы по вызову в обход препятствий в виде слабого регулирования или его отсутствия, не должна остаться незамеченной.

Представляется, что цифровые технологии так или иначе способствуют выходу работы по вызову за рамки трудовых отношений. Расплывчатым в современной реальности выглядит самое понятие, которое ассоциируется уже не только со сферой наемного труда. Формы нестандартной занятости, которые более экономически привлекательны, где меньше рисков и издержек, претендуют занять нишу работы по вызову. В связи с ростом гибкости и дестандартизации некоторые страны пытаются выработать подходы, которые покрывали бы различные ситуации нестандартной занятости и повышали в первую очередь гибкость трудовых отношений по найму. Одним из решений, например, в Нидерландах выбрана работа по вызову [17. С. 23–24].

В исследовании Европейского фонда по улучшению условий труда и жизни (далее – Еврофонд) 2015 г. новые формы занятости условно разделены на две группы: те, что предполагают новые модели трудовых отношений, и те, что предполагают новые модели работы [3]. Указание на то, что формы и модели новые, также условно, потому что они могут быть как ранее неизвестные, так и модифицированные и (или) приобретающие все большее значение в Европе. Casual work (временная, случайная, разовая работа) – работа нестабильная и непродолжительная, по мнению экспертов Еврофонда, является новой моделью работы, работой по требованию. Новизна здесь связана со все большим распространением такой работы в разных странах и непрекращающимся поиском эффективного регулирования.

Различают два типа casual work: intermittent work (работа «время от времени» («от случая к случаю»)) и on-call work (работа по вызову). Работа по вызову – длящиеся трудовые отношения, но время, когда работник не привлекается к работе, по общему правилу не оплачивается. Суть такой работы заключается в том, что работодатель привлекает работника к работе по мере необходимости, что исклю-

чает возможность заранее определить время работы, до начала работы работник находится в режиме ожидания вызова на работу. Еврофонд выделяет два ставших уже классическими вида трудовых договоров о работе по вызову, которые могут быть срочными или бессрочными: трудовой договор с минимальным (сколько работодатель должен предоставить) и максимальным (сколько работник должен отработать) количеством рабочих часов (min-max contracts) и трудовой договор без указания рабочих часов (zero-hours contracts).

Судя логике Еврофонда, работа по вызову, особенно при трудовых договорах «ноль часов», является той же работой «время от времени», разница лишь в том, что резерв дежурных работников на экстренную замену или на случай увеличения объема работы заранее определен работодателем. У экспертов МОТ видение немного другое. В упомянутом обзоре работа «время от времени», в том числе работа по дням, включена в укрупненную группу «Временная занятость» (срочные трудовые договоры), а работа по вызову отнесена к укрупненной группе «Работа на неполное рабочее время и работа по вызову» (трудовые договоры с укороченными рабочими часами). По мнению МОТ, занятость на условиях неполного рабочего времени не только приобрела важное значение, но и стала более разнообразной и теперь включает в себя работу по вызову, для которой характерны короткая продолжительность рабочего времени или отсутствие стабильного графика работы [15. С. 14].

Практика работы по вызову реализуется в США, Великобритании, Ирландии, Мексике, Германии, Финляндии, Италии, Нидерландах, Швеции, Турции и других странах. Несмотря на то, что в зарубежных странах уже накоплен определенный опыт регулирования работы по вызову, есть сомнения, что достигнутый уровень экспертизы достаточен для выработки универсальных стандартов, что подтверждается, в том числе их отсутствием на уровне МОТ, которая пока ограничивается общими рекомендациями. МОТ считает, что для защиты работников по вызову могут быть применены меры, обеспечивающие гарантированное минимальное количество рабочих часов, а также меры, позволяющие работникам влиять на график работы, включая введение ограничений на одностороннее изменение рабочего времени [15. С. 26].

Неустойчивый характер работы по вызову обусловлен отсутствием гарантий работы, непредсказуемостью рабочего времени и, соответственно, вознаграждения, при этом на работника налагаются ограничения в части распоряжения временем, когда работа не выполняется. Последнее и отсутствие заранее установленного графика работы придает специфику работе по вызову и позволяет выделить ее среди других способов организации труда. Выявление природы времени без работы и его пределов позволит определиться с понятием работы по вызову, а также выработать механизм снижения прекаризационных рисков при ее организации. Проблема в том, что специфика работы по вызову, а значит, интерес к ней, сохранятся только тогда, когда время без работы не будет оплачиваться либо выплата компенсации за ограничение свободы работника будет экономически выгодна.

Разрешить противоречия, вероятно, не так просто, раз бороться со злоупотреблениями страны пытаются через запрет работы по вызову, лимитирование

резерва дежурных работников, часов работы или возрастные ограничения, конвертацию договора в бессрочный на полный рабочий день (например, в Италии лимит составляет до 400 часов на каждого работника в течение трех лет, на работу могут быть приняты работники в возрасте до 25 и старше 55 лет). Производятся попытки решать вопрос с гарантией работы. Например, вызов на работу не менее чем на 3 часа (Германия, Бельгия), на 4 часа (Турция). Предпочтительны договоры с минимальными часами (10, 15, 20 часов в неделю). Но все это лишь позволяет работнику при отсутствии работы получить компенсацию из расчета данных часов, но не саму работу. Компенсация, кстати, возможна при «нулевых» договорах. В частности, в Ирландии при отсутствии работы работник имеет право на компенсацию не менее чем за 15 часов или 25% от суммы договора.

В 2022 году Кодекс законов о труде Украины дополнен статьей 21.1, урегулировавшей трудовые отношения с нефиксированным рабочим временем [8]. Работа по вызову на Украине – это трудовой договор с нефиксированным рабочим временем, заключение которого данным работодателем ограничено (не более 10 % от общего количества трудовых договоров, для работодателей – физических лиц, использующих труд менее 10 работников, – не более 1). При заключении такого договора стороны должны договориться не только о порядке вызова на работу, но и о времени, когда можно потребовать выход работника на работу (базовые часы и дни). Базовые часы не могут превышать 40 часов в неделю, а базовые дни – 6 дней в неделю. Минимально гарантированные часы – 32 часа в месяц. При отсутствии работы или работы в меньшем объеме работник получает заработную плату из расчета 32 часов. После 12 месяцев работы работник вправе впервые обратиться к работодателю с требованием заключить срочный или бессрочный трудовой договор с графиком работы. Повторное обращение возможно не ранее чем через 90 дней со дня получения отказа.

Таким образом, при работе по вызову время без работы, как правило, в рабочее время не включается и не оплачивается. Оплата может быть, конечно, предусмотрена в соглашении (Италия), время ожидания может оплачиваться, но только если работник находится на территории работодателя (Великобритания). Редкий случай, когда время без работы зафиксировано в законе (Украина), что правильно, поскольку время ожидания вызова на работу охвачено действием трудового договора и должно быть определенным, работник обязан приступить к работе при наличии требования работодателя в этот период времени. Правда, есть практика избежания данной обязанности посредством заключения «рамочных трудовых соглашений», когда работник может отказаться от работы без каких-либо последствий, потому что каждый вызов на работу сопровождается заключением срочного трудового договора (такой вид соглашений о работе по вызову применяется в Нидерландах). Подобную практику можно назвать квазиработой по вызову.

В связи с распространением дежурной работы в Европе рассматривается возможность введения третьей, промежуточной между рабочим временем и временем отдыха, категории – времени нахождения в состоянии готовности, которое может быть активным и неактивным [26. С. 34]. Следует заметить, что время нахождения в состоянии готовности не связывается с работой по вызову. В Финляндии сторо-

ны могу договориться о дежурстве за выплату компенсации, за исключением тех работ, где дежурство обязательно. Время ожидания работы будет рассматриваться как рабочее время, если требуется присутствие на рабочем месте или в непосредственной близости от него [5]. Дежурство за рамками графика работы допускается в Словакии. Работодатель может требовать от работника ожидать вызова на работу сверхурочно или в выходной день в течение максимум 8 часов в неделю и 100 часов в календарный год. Дежурства свыше этих часов возможны с согласия работника в пределах ограничений, которые могут быть предусмотрены в коллективном договоре. Время нахождения вне рабочего места является неактивной частью рабочей готовности и в рабочее время не включается, но в этом случае работнику выплачивается компенсация не менее 20% минимальной заработной платы [23].

В России слабое правовое регулирование дежурств. Общими правилами можно назвать положения постановления Секретариата ВЦСПС от 02.04.1954 № 233 «О дежурствах на предприятиях и в учреждениях», которое применяется в части не противоречащей Трудовому кодексу Российской Федерации (далее – ТК РФ) [1]. По смыслу постановления время дежурства является рабочим временем, оно пропорционально компенсируется временем отдыха на следующий день, если дежурить пришлось после окончания рабочего дня, или в течение 10 дней при дежурстве в выходные и праздничные дни. Дежурства вне рабочего места на уровне ТК РФ были урегулированы в 2013 году применительно к медицинским работникам, тогда как по факту они предусмотрены и для других профессий (например, спасателей, некоторых работников железнодорожного транспорта общего пользования).

Согласно статье 350 ТК РФ, дежурство – ожидание вызова на работу. Ожидать вызова на работу медицинские работники могут только дома (таким образом, достаточно невнятно обозначено место, которое находится, по мнению законодателя, близко к работе). В соответствии с Положением об особенностях режима рабочего времени и учета рабочего времени при осуществлении медицинскими работниками медицинских организаций дежурств на дому, утвержденному приказом Минздрава России от 02.04.2014 № 148н [19], время дежурства определяется графиком работы. Время дежурства учитывается в размере 1/2 часа рабочего времени за каждый час дежурства и при необходимости корректируется, чтобы не нарушалась норма рабочего времени за учетный период. При вызове на работу время следования до места работы и время оказания медицинской помощи учитывается как час рабочего времени.

В немногочисленных исследованиях, где уделялось внимание работе по вызову, утверждается, что это нетипичный режим рабочего времени [29, С. 119], режим гибкого рабочего времени [16. С. 88]. Некоторые авторы гибким режимом при неполном рабочем времени, но не работой по вызову, считают договоры «минимум-максимум» [12. С. 83; 4. С. 307]. М.А. Шабанова и Н.Р. Никитина полагают, что в России применение практики работы по вызову возможно и она даже имеется. Возможность введения такой практики при ряде условий и ограничений допускает А. Е. Коркин. Н. В. Закалюжная придерживается мнения, что «работа по вызову не может быть применена в российском праве, поскольку не укладыва-

ется в существующую концепцию трудовых отношений». Без формализованных признаков явления сложно подтвердить или опровергнуть его наличие, но, глядя на нормы о дежурстве, следует признать, что определенный задел в регулировании уже имеется.

МОТ под рабочим временем понимает период, в течение которого работники находятся в распоряжении нанимателя [9]. Согласно статье 91 ТК РФ, в структуру рабочего времени входит время, в течение которого работник должен исполнять трудовые обязанности, а также иные периоды времени. Какие периоды времени включать в рабочее время, определяет регулятор. Очевидно, что речь идет о периодах времени, когда работник трудовую функцию не выполняет, но продолжает находиться в той или иной степени под управлением работодателя, в том числе обязан реагировать на его обращения. Время, охваченное трудовым договором (рабочее время), имеет пределы, определяемые нормой рабочего времени. В случае работы по вызову структура рабочего времени представлена двумя периодами: время работы и время нахождения в состоянии готовности (время ожидания вызова на работу).

Оба периода времени при работе по вызову являются плавающими, но в любом случае не должны в сумме выходить за пределы нормы рабочего времени. Получается, что работа по вызову – особый способ организации труда, при котором структура рабочего времени является двукомпонентной и гибкой. При работе сверхурочно, работе в выходной или нерабочий праздничный день происходит выход на пределы нормы рабочего времени, но и он имеет границы. В пределах данных границ двукомпонентная гибкая структура рабочего времени сохраняется. По факту, особый способ организации труда может быть применен, когда структура рабочего времени специфична полностью или в какой-то части, поэтому предложения внести изменения в ст. 91 ТК РФ не лишены смысла [26. С. 41]. Размышления эти отвергаются [12. С. 75–76], но кажется, что такой подход позволяет применять особый способ организации труда даже безотносительно к виду работы (например, работа по совместительству, дистанционная (удаленная) работа).

Повышение уровня определенности – действенный способ снижения прекаризационных рисков. При работе по вызову приблизиться к балансу между экономической эффективностью и социальной справедливостью можно посредством не только очерчивания, но и адекватной оплаты времени ожидания. Справедливым видится учет времени ожидания вызова на работу в размере не менее одной четвертой часа рабочего времени за каждый час ожидания. Это время может быть увеличено в зависимости от ограничений работника по месту нахождения и времени реагирования на вызов. В российских социально-экономических и правовых условиях данный подход более приемлем, нежели оплата рабочих часов без их реальной отработки или выплата компенсации, не говоря уже об игнорировании какого-либо вознаграждения, когда у работодателя полностью отсутствует стимул работу предоставить.

Программой сотрудничества между Российской Федерацией и Международной организацией труда на 2021–2024 гг. [30] предусмотрено содействие переходу от неформальной занятости к формальной. Без указания на скорей-

шую модернизацию трудового законодательства, но согласно программе предполагается с целью расширения возможностей занятости изучение международных практик регулирования нестандартных форм занятости, включая агентскую, удаленную, комбинированную, временную, частичную и платформенную занятости. Что это, если не подвижки, первые шаги в сторону оптимального регулирования, которое должно создать реальные условия, поддерживающие конкуренцию моделей стандартной и нестандартной занятости [24. С. 26], хотя научная общественность оптимизма по поводу легализации в России работы по вызову не разделяет.

Н. Л. Лютов утверждает, что выведение работы по вызову из сферы неформальной занятости не компенсирует несправедливости данной формы трудовых отношений и нестабильности занятости, повышает риски замещения классических трудовых отношений «разовой» занятостью, поэтому легализация такой практики в России нецелесообразна [24. С. 101]. Менее категорична позиция Л. А. Чикановой и Л. В. Серегиной, которые считают, что «отсутствие правового регулирования таких форм труда создает неопределенность правового статуса работающих, что свидетельствует о незащищенности их труда, в том числе от безработицы», и более того предлагают включить в ТК РФ специальный раздел о трудовой деятельности в нетипичных (нестандартных) формах занятости [22. С. 500–502]. Ранее М. А. Шабанова предлагала редакцию специальной главы о работе по вызову [29. С. 138–141], а Н. Р. Никитина главы об особенностях регулирования работы в режиме гибкого рабочего времени с отдельной статьей о работе по вызову [16. С. 151–157].

Представляется, что, несмотря на тонкие места и даже серые зоны, у работы по вызову есть будущее, запрос на такую работу очевидно имеется. Кроме того, еще больше раскрыть потенциал работы по вызову, одновременно сделав ее прозрачной и управляемой, помогут цифровые технологии. С 2013 года в Великобритании существует платформа Slivers of Time, изначально используемая для волонтеров, затем ориентированная на разовую работу. С помощью платформы находят друг друга и взаимодействуют работодатели и работники, готовые работать несколько часов в неделю. В России постоянно совершенствуется функционал платформы «Работа России». В августе 2023 года Минтруд России предложил создание на платформе нового сервиса для размещения и подбора разовых заданий и работ, а также заключения гражданско-правовых договоров в электронном виде. Аналогичный сервис может быть запущен и для работы по вызову, что выглядит не менее приоритетным и значимым социально ориентированным действием, чем специальные налоговые режимы и распространение социальной защиты на лиц, заключивших гражданско-правовые договоры.

Список литературы

1. Постановление Секретариата ВЦСПС от 02.04.1954 № 233 «О дежурствах на предприятиях и в учреждениях» // Бюллетень ВЦСПС. 1954. № 8

2. Долженко Р. А., Попов Э. И. Взаимосвязь новых форм трудовых отношений и прекаризации труда в постиндустриальной экономике // Вестник Алтайского государственного аграрного университета. 2014. № 12(122). С. 179–185.

3. Европейский фонд улучшения условий жизни и труда. URL: https://www.eurofound.europa.eu/publications/report/2015/new-forms-of-employment#tab-01

4. Закалюжная Н. В. Основные формы нетипичных трудовых отношений в России и за рубежом в условиях модернизации экономики: дис. … д-ра юрид. наук. М., 2021. 433 с.

5. Закон Финляндии «О рабочем времени». URL: https://www.finlex.fi/sv/laki/ajantasa/2019/20190872

6. Кастель Р. Метаморфозы социального вопроса. Хроника наемного труда / пер. с фр.; общ. ред. ред. пер. Н. А. Шматко. СПб.: Алетейя, 2009. 574 с.

7. Киселев И. Я. Зарубежное трудовое право: учебник для вузов. М.: ИНФРА-М, 1998. 263 с.

8. Кодекс законов о труде Украины. URL: https://online.zakon.kz

9. Конвенция № 30 Международной организации труда «О регламентации рабочего времени в торговле и в учреждениях» (г. Женева 28.06.1930) // Конвенции и рекомендации, принятые Международной конференцией труда. 1919-1956. Т. I. Женева: Международное бюро труда, 1991. С. 213-218.

10. Котляров И. Д. Проблемы регулирования нестандартных форм занятости // Journal of Economic Regulation. 2015. Т. 6, № 1. С. 55-66.

11. Котова С. И. Правовое положение прекариата на рынке труда и концепция занятости: дис. … канд. юрид. наук. М., 2019. 206 с.

12. Коркин А. Е. Отношения по применению нетипичного труда: понятие, виды, общие вопросы правового регулирования: дис. … канд. юрид. наук. СПб., 2012. 224 с.

13. Масленникова Е. В., Колесник Е. А., Антонова О. А. Исследование форм нестандартной занятости в контексте реализации признаков достойного труда // Вестник Омского университета. Серия: Экономика. 2022. Т. 20, № 1. С. 102-114.

14. Международная организация труда [сайт]: URL: https://www.ilo.org/global/research/global-reports/weso/WCMS_865332/lang--en/index.htm

15. Международная организация труда [сайт]: URL: https://www.ilo.org/global/publications/books/WCMS_554952/lang--en/index.htm

16. Никитина Н. Р. Режим рабочего времени и его виды (правовой аспект): дис. … канд. юрид. наук. Москва, 2011. 170 с.

17. Платформенная занятость: определение и регулирование / О. В. Синявская, С. С. Бирюкова, А. П. Аптекарь, Е. С. Горват, Н. Б. Грищенко, Т. Б. Гудкова, Д. Е. Карева; Национальный исследовательский университет «Высшая школа экономики», Институт социальной политики. – М.: НИУ ВШЭ, 2021. 77 с.

18. Попов А. В., Соловьева Т. С. Прекаризация занятости: анализ научного дискурса о сущности и векторах измерения // Социологические исследования. 2020. № 9. С. 103-113.

19. Российская газета. 2014. № 117.

20. Стэндинг Г. Прекариат: новый опасный класс. М.: Ад Маргинем Пресс, 2014. 328 с.

21. Трансформация трудовых отношений: факторы социального загрязнения: кол. монография / под ред. А. Э. Федоровой. Екатеринбург: ЮНИКА, 2019. 178 с.

22. Трудовое право: национальное и международное измерение: монография. Т. 1 / под ред. С. Ю. Головиной, Н. Л. Лютова. М.: Норма, 2022. 608 с.

23. Трудовой кодекс: Закон Словацкой Республики от 02.07.2001 № 311 (заглавие с экрана). URL: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2001/311/

24. Трудовые отношения в условиях развития нестандартных форм занятости: монография / под ред. Н. Л. Лютова, Н. В. Черных. М.: Проспект, 2022. 256 с.

25. Хныкин Г. В. Прекариат как субъект трудовых отношений // Законодательство. 2019. № 2. С. 34-39.

26. Чанышев А. С. Правовое регулирование рабочего времени и времени отдыха в странах Скандинавии: монография. М.: Проспект, 2016. 128 с.

27. Черепанцева Ю. С. Прекариат и его влияние на развитие трудовых отношений // Труды Оренбургского института (филиала) Московской государственной юридической академии. 2017. № 31. С. 140-145.

28. Чичина Е. В. Нестандартная занятость: к вопросу о терминологической неопределенности // Цифровые технологии и право: сборник научных трудов I Международной научно-практической конференции (г. Казань, 23 сентября 2022 г.) / под ред. И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой. В 6 т. Т. 3. Казань: Изд-во «Познание» Казанского инновационного университета, 2022. 440 с.

29. Шабанова М. А. Особенности правового регулирования нетипичных трудовых договоров: дис. … канд. юрид. наук. Ярославль, 2008. 211 с.

30. Программа сотрудничества между РФ и МОТ 2021–2024. URL: https://mintrud.gov.ru

С. А. Петрова,
кандидат педагогических наук,
Самарский университет государственного управления
«Международный институт рынка»

К ВОПРОСУ О ЦИФРОВИЗИАЦИИ ТРУДОВЫХ И ИНЫХ НЕПОСРЕДСТВЕННО СВЯЗАННЫХ С НИМИ ОТНОШЕНИЙ

Аннотация. Цифровизация экономики кардинальным образом повлияла на правовую природу трудовых отношений. Помимо традиционных трудовых отношений, стали востребованными самозанятые, а также работа на интернет-платформе. В статье рассматривается развитие регулирования электронного документооборота в трудовых отношениях в России, а также намечены перспективные направления развития цифровизации трудовых и иных непосредственно связанных с ними отношений в Российской Федерации.

Ключевые слова: цифровизация, трудовые отношения, электронный документооборот, интернет-платформа, самозанятые, охрана труда

ON THE ISSUE OF DIGITALIZATION OF LABOR AND OTHER DIRECTLY RELATED RELATIONS

Abstract. The digitalization of the economy has radically affected the legal nature of in the labor relations. In addition to traditional labor relations self-employed people have become in demand, as well as work on an Internet platform. The article deals with the development of the regulation of electronic document management in labor relations in Russia and also outlines promising directions for the development of digitalization of labor and other directly related relations in the Russian Federation.

Keywords: digitalization, labor relations, electronic document management, Internet platform, self-employed, labor protection

Информационные технологии продолжают активно входить в повседневную жизнь каждого. Не секрет, что цифровизация направлена на то, чтобы повысить эффективность рабочих процессов, а также сделать жизнь каждого работника и работодателя более эффективной, мобильной, экономичной [5. С. 30].

Сегодня активно развивается и совершенствуется в сфере трудовых и непосредственно связанных с ними отношений ведение электронного документооборота, включая ведение сведений о трудовой деятельности работников, регулирование труда дистанционных работников [3. С. 5].

На наш взгляд, в сфере трудовых и иных непосредственно связанных с ними отношений можно наметить следующие перспективные направления развития цифровизации:

– дальнейшее совершенствование функционала цифровой платформы «Работа в России» [2. С. 49]. Так, продолжение развития и совершенствования автоматизированного контроля за деятельностью работодателя позволит снизить риск правонарушений еще на стадии принятия решений и разработки кадровых документов, а размещение на данной цифровой платформе готовых моделей/образцов решений и документов будет содействовать повышению правовой культуры кадровых работников, а также позволит сократить время на работу с документами и, как следствие, повысить производительность труда [1. С. 12]. Необходимо подчеркнуть, что продолжение развития электронного взаимодействия сторон трудового договора позволит сделать трудовые отношения прозрачными, более понятными для сторон, а также гарантирует длительное хранение документов и является залогом соблюдения работодателем прав работников [4. С. 116];

– включение такой категории, как «самозанятые», в понятийный аппарат Трудового кодекса Российской Федерации, в качестве отдельной особой категории [7. С. 44].

Считаем, что разработка правовых норм, регламентирующих их занятость, должна проводиться именно Трудовым кодексом Российской Федерации, в котором отдельная глава может быть посвящена их трудовым правам и обязанностям, а также закреплению социальных гарантий;

– регламентация и включение в Трудовой кодекс Российской Федерации отношений между интернет-платформой и работником [6. С. 44]. Закрепление таких трудовых отношений возможно, на наш взгляд, как разновидность дистанционной

работы, и это позволит для такой категории работников законодательно установить связанные с режимом рабочего времени, времени отдыха, оплатой труда, социального страхования, охраной труда и иными гарантиями для таких работников;

– охрана труда и расследование несчастных случаев с дистанционными работниками, работниками интернет-платформы, самозанятыми.

На наш взгляд, необходимо на законодательном уровне четко определить критерии для установления факта трудовых отношений между интернет-платформой и работником.

Итак, дальнейшее развитие экономики России и активное внедрение во все сферы общественной жизни цифровизации позволит внести в трудовое законодательство ряд новаций и изменений, которые стимулируют дальнейшее развитие трудовых и иных непосредственно связанных с ними отношений.

Список литературы

1. Бережнов А. А. Цифровизация в сфере труда и ее влияние на повышение производительности труда // Трудовое право в России и за рубежом. 2022. № 2. С. 11-13.

2. Кондратенко А. М., Гиряева В. Н. Регулирование электронного документооборота по трудовому праву России: актуальное состояние и перспективы развития // Трудовое право в России и за рубежом. 2022. № 3. С. 48-51.

3. Крылов К. Д. Современная трансформация российского и международного трудового права // Трудовое право в России и за рубежом. 2022. № 4. С. 3-6.

4. Кудашкин А. В., Потапов А. В. О внедрении электронного документооборота в трудовых отношениях // Оборонно-промышленный комплекс: управление, экономика и финансы, право. 2022. № 2. С. 111-117.

5. Лушников А. М. Цифровизация трудового права и трудовые отношения // Закон. 2022. № 10. С. 28-37.

6. Лушников А. М., Лушникова М. В. Современное российское трудовое право: глобальные вызовы в контексте риска и неопределенности // Трудовое право в России и за рубежом. 2023. № 1. С. 2-5.

7. Сапфирова А. А. Правовое регулирование самозанятости и работы на платформах в условиях цифровой экономики: трудовой и (или) гражданско-правовой аспекты? // Гражданское право. 2021. № 5. С. 41-45.

С. П. Пшеничный,
старший преподаватель,
Казанский (Приволжский) федеральный университет

ПЕРСПЕКТИВЫ РЕГУЛИРОВАНИЯ СОЦИАЛЬНОГО ПАРТНЕРСТВА В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Аннотация. В статье проводится анализ изменений во взаимодействии субъектов системы социального партнерства на разных этапах его существования. Особое внимание уделяется регулированию взаимоотношений работодате-

лей, наемных работников и государства в контексте развития гибких форм занятости, в том числе платформенной занятости в условиях цифровой трансформации. Целью исследования является проведение анализа характеристик складывающейся системы взаимодействия и обоснования направлений ее совершенствования.

Ключевые слова: социальное партнерство, цифровая трансформация, платформенная занятость, самозанятость, гибкая занятость, уровни социального партнерства, коллективный договор

PROSPECTS FOR REGULATING SOCIAL PARTNERSHIP IN THE CONTEXT OF DIGITAL TRANSFORMATION

Abstract. The article analyzes changes in interactions between subjects of the social partnership system at different stages of its existence. Particular attention is paid to regulating mechanism of the state, employers and employees relationship in the context of flexible forms of employment, including platform employment in digital transformation conditions. The research aim is to analyze the characteristics of the interaction system and to justify the improvement directions.

Keywords: social partnership, digital transformation, platform employment, self-employment, flexible employment, levels of social partnership, collective agreement

Введение. Развитие экономики в современных реалиях сопряжено с внедрением в жизнь цифровых технологий, которые вызывают кардинальные изменения общественных отношений, контуров рынка труда, трансформацию институтов образования, медицинского и пенсионного обеспечения. Под влиянием процессов цифровизации экономики происходит развитие новых форм занятости, включающих в себя дистанционную занятость, самозанятость и платформенную занятость, представляющих основной тренд, влияющий на рынок труда, изменяющиеся интересы, возникающие противоречия и механизмы их разрешения.

Обозначенные вопросы в условиях классических трудовых отношений, как правило, решаются через институт социального партнерства, позволяющий учесть интересы представителей различных групп, влияющих на развитие трудовых отношений. Наиболее известной формой социального партнерства является участие в коллективных переговорах по подготовке проектов и заключению коллективных договоров и соглашений. Однако, анализируя специфику новых форм занятости, можно выдвинуть гипотезу, что необходимо внести существенные коррективы в функционирование данного института для сохранения его эффективности.

Основная часть. Развитие социального партнерства в России берет свое начало с 1906 года, с момента появления первых профсоюзных организаций [8. С. 47]. Справедливо выделить несколько основных периодов развития социального партнерства: с 1906 по 1917 г. – время появления первых тарифных соглашений; с 1917 по 1990 г. – отсутствие коллективно-договорного регулирования социально-трудовых отношений, связанное с развитием командно-административной экономики; с 1991 г. по настоящее время – стадия активного развития социального партнерства и его институциализации. В рамках последнего из выделенных периодов в ст. 23

Трудового кодекса Российской Федерации (далее – ТК РФ) само явление социального партнерства было определено следующим образом: «Социальное партнерство в сфере труда (далее – социальное партнерство) – система взаимоотношений между работниками (представителями работников), работодателями (представителями работодателей), органами государственной власти, органами местного самоуправления, направленная на обеспечение согласования интересов работников и работодателей по вопросам регулирования трудовых отношений и иных непосредственно связанных с ними отношений» [9]. Обозначенный этап является наиболее интересным с точки зрения прослеживания современных тенденций в регулировании взаимоотношений работодателей, наемных работников и государства и позволяет выделить внутри него несколько этапов.

Первый из этапов, в рамках которого создавая систему социального партнерства государство рассматривало возможность переложить часть полномочий по обеспечению социальных гарантий населению на бизнес-сообщество, стартовал 15 ноября 1991 г. [5]. Взаимодействие государства и представителей наемных работников в указанный период существенно отличалось от того, как оно складывалось ранее во времена СССР, когда государство одновременно являлось и гарантом социальной стабильности, и работодателем. Предприниматели же воспринимали происходящее как дополнительный скрытый налог и не были заинтересованы в участии в этом процессе. В научной среде велась активная дискуссия, посвященная осмыслению вопросов построения системы реализации интересов бизнеса, государства и наемных работников в рамках социального партнерства, а также разработке понятийного аппарата [7, 8].

Период 2003–2006 годов в развитии социального партнерства связан с имплементацией механизмов коллективно-договорного регулирования как эффективного механизма согласования социально-экономических интересов. Дальнейшее развитие социального партнерства характеризуется совершенствованием элементов социально-экономического института как фундамента для регулирования интересов в социально-трудовой сфере. Начало последнего на данный момент периода развития социального партнерства, связанного с развитием традиционных форм занятости, относится к 2009 году. В этот период исследователи обратили внимание на возможность использования потенциала социального партнерства не только как института регулирования социально-трудовых отношений, но и включения новых субъектов, таких как некоммерческие организации и социальные предприниматели, в процесс реализации интересов [7, 8].

Несмотря на активное развитие социального партнерства в России, что с точки зрения нормативного регулирования безусловно характеризуется системностью в заключении договоров и соглашений на разных уровнях партнерства, анализируя этапы развития социального партнерства, можно сделать вывод о сформированности следующих проблем, снижающих эффективность его использования как социально-экономического института.

В научных трудах, посвященных развитию социального партнерства в России, обозначается ряд проблем, характерных для системы социального партнерства. Первая из них – необходимость существенного повышения статуса ор-

ганов социального партнерства, реализация принципа равенства сторон, а также последовательное повышение во всех отраслях и секторах экономики доли работников, охваченных коллективно-договорными механизмами регулирования социально-трудовых отношений. Можно отметить, что норма ТК РФ об участии органов социального партнерства в формировании и реализации государственной политики в сфере труда не в полной мере реализуется на практике, что приводит к конфликту интересов и снижению эффективности взаимодействия в рамках системы социального партнерства. Также осуществлению эффективного диалога партнеров препятствует несформированность субъектов социального партнерства на большинстве малых и средних предприятий реального сектора экономики, низкая социальная ответственность работодателей, их нежелание брать на себя обязательства по достойной оплате труда, продуктивной занятости, обучению персонала и социальным гарантиям [7, 8].

Цифровизация экономики приводит к изменению социальных взаимосвязей в обществе, существенно влияя на порядок организации взаимодействия между людьми в целом, между наемными работниками, работодателями и государством. Основным фактором, влияющим на этот процесс, является возможность существенного снижения трансакционных издержек при внедрении цифровых технологий. Использование современных технологий существенно снижает затраты на поиск и обработку информации, согласование позиций сторон взаимодействия и заключения договоров.

В условиях цифровой трансформации одним из драйверов которой сфера трудовых отношений в России стала эпидемия Covid-19, можно наблюдать, как проявляются несколько форм занятости – дистанционная занятость, когда работник выполняет свою трудовую функцию не находясь непосредственно на территории работодателя, но имея заключенный с ним трудовой договор, а также самозанятость и платформенную занятость, когда фактически такой договор отсутствует. Исследования показывают, что бизнес видит преимущества от цифровизации трудовой сферы и нацелен на расширение масштабов применения дистанционной и других гибких форм занятости [3. С. 48]. Стоит отметить, что с появлением новых форм занятости у экономических субъектов происходит изменение в развитии потребностей, связанных с формированием и использованием человеческого капитала, однако в условиях неурегулированности взаимоотношений на законодательном уровне наблюдается снижение уровня социальной защищенности. Востребованность новых форм занятости на рынке труда явилась катализатором процесса кодификации ряда положений, регулирующих применение таких форм. В частности, регулирование дистанционной занятости нашло свое отражение в рамках положений главы 49.1 ТК РФ [9].

В 2023 году в Государственную Думу был внесен законопроект № 275599-8, предлагающий новую редакцию Федерального закона «О занятости населения в Российской Федерации» [3]. В частности, в пунктах 3 и 4 статьи 2 законопроекта дается законодательное определение понятиям «самозанятость» и «платформенная занятость». Таким образом, можно отметить, что делается попытка на законодательном уровне отрегулировать новые формы трудовых отношений, возникшие в том числе

под влиянием процессов цифровизации экономики. По состоянию на сентябрь 2023 года предлагаемый законопроект принят Государственной Думой в первом чтении.

Внесение в законодательство обозначенных выше изменений дает работодателям основания для расширения спектра предоставляемых услуг в части социальной защиты работников и позволяет компаниям привлекать, а затем и удерживать наиболее эффективных сотрудников, предоставляя им возможности для повышения качества их трудовой жизни. Развитие цифровых технологий позволяет кастомизировать меры социальной поддержки предоставляемой компанией для каждого сотрудника, делая их более уникальными и тем самым повышая привлекательность компании в лице нанятых и потенциальных сотрудников. Для развития экономики наиболее важными способностями, которыми должны обладать современные сотрудники, являются компетенции, обеспечивающие динамическое развитие и инновационный рост компаний [7. С. 437]. Безусловно, формированию этих компетенций способствует выстраивание постоянного процесса обучения сотрудников, сохранение высокого уровня здоровья, комфортной рабочей среды и высокого уровня социальной защищенности независимо от территориального расположения сотрудников относительно работодателя. На рис. 1 представлены, на наш взгляд, наиболее перспективные направления в условиях цифровизации экономики, в рамках которых необходимо развивать деятельность в сфере социального партнерства, в том числе реализовывать меры, направленные на обеспечение законодательного регулирования этих сфер деятельности.

По итогам июля 2023 года количество самозанятых в России составило 8,062 млн, увеличившись в 1,2 раза, или на 1,5 млн, по сравнению с данными регистрации на конец 2022 года [4]. Принимая во внимание приведенную статистику, а также в контексте актуальности построения в компаниях территориально распределенных команд, вопрос предоставления сотрудникам, работающим в условиях гибких форм занятости, социальных гарантий, предусмотренных, в частности, в рамках коллективных договоров и позволяющих реализовать принцип равенства всех сотрудников компании, встает достаточно остро.

Интересными примерами реализации концепции социального партнерства в рамках платформенной занятости могут служить проекты, реализованные датской платформой Hilfr.dk и российской YouDo. В рамках первого Hilfr.dk подписала коллективный договор с профсоюзом 3F. Соглашение позволило работникам платформы получить единые согласованные условия по выплатам, а также возможность занятых выбирать, хотят ли они квалифицироваться в качестве официальных сотрудников или оставаться фрилансерами [6]. Предложение платформы YouDo, реализованное в период первой волны заболеваемости Covid-19, заключалось в возможности для исполнителей, зарегистрированных на платформе, перенести болезнь дома, восстанавливая здоровье, и получить при этом минимальный заработок. Оформить услугу страхования здоровья исполнитель мог при пополнении баланса или покупке пакета откликов на сайте YouDo. Инициатива платформы была реализована в партнерстве со страховыми компаниями. Кроме этого, YouDo продумывает возможность аналогичных решений для создания пенсионной программы для исполнителей в партнерстве с ведущими пенсионными фондами [10].

Рис. 1. Направления развития социального партнерства в условиях цифровой трансформации

Повсеместное применение цифровых технологий позволяет эффективно организовать процесс предоставления социальных услуг сотрудникам и обеспечить согласование интересов работников и работодателей по вопросам регулирования трудовых отношений и иных непосредственно связанных с ними отношений. Развитость цифровых платформ, основной целью деятельности которых является предоставление возможности «потребителям и поставщикам связываться онлайн для обмена продуктами, услугами и информацией» [2. С. 99], позволяет довольно быстро и гибко подобрать поставщиков услуг, востребованных конкретным сотрудником и зафиксированных в коллективном договоре независимо от территории его присутствия.

Другим инструментом, позволяющим сократить трансакционные издержки в процессе реализации соглашений, заключенных на уровне компаний в рамках социального партнерства, являются системы электронного документооборота, получившие широкое распространение. Указанный механизм позволяет реализовать как непосредственно механизм официального оформления трудовых отношений между субъектами, обеспечить вовлеченность работников в процесс заключения коллективных договоров как на уровне предприятия, так и на уровне трехсторонних комиссий, а также непосредственную реализацию интересов каждой из сторон социального партнерства.

Заключение. В рамках исследования рассмотрены два принципиально разных варианта трудовых отношений, которые в равной степени будут представлены в условиях цифровой трансформации и потребуют их детальной регламентации в рамках трудового законодательства. Специфика каждого из видов трудовых отношений и их применимость для реализации экономических интересов работодателей, наемных работников и государства показала эффективность каждого из них. Выявленные в статье наиболее важные компетенции, которыми должны обладать сотрудники компаний в условиях цифровой трансформации и на формирование которых непосредственно влияет степень реализации социальной политики компании, указывают на актуальность применения механизма социального партнерства. Определены перспективные направления развития института соци-

ального партнерства, включающие в себя программы дополнительного профессионального обучения и медицинского страхования, создание комфортной рабочей среды и высокого уровня социальной защищенности. Необходимость глубокого законодательного регулирования обозначенных направлений в контексте протекания в России процессов цифровой трансформации является актуальным вопросом, который должен быть решен в ближайшей перспективе.

В статье обозначены проблемы, с которыми столкнулся институт социального партнерства на более ранних периодах своего развития, анализируя которые необходимо отметить, что для повышения эффективности института социального партнерства необходима реализация принципа равенства сторон, а также последовательное повышение во всех отраслях и секторах экономики доли работников, охваченных коллективно-договорными механизмами регулирования социально-трудовых отношений. Использование современных инструментов выстраивания коммуникации, получивших широкое распространение в условиях цифровой трансформации позволяет достичь указанных целей.

Список литературы

1. Гонтар Е. А. Тренды рынка труда в контексте цифровизации экономики // XXXV International Plekhanov Readings : Юбилейный сборник статей аспирантов и молодых ученых на английском языке. Москва, 25 марта 2022 года. М.: Российский экономический университет имени Г. В. Плеханова, 2022. С. 47-51.

2. Жевняк О. В. Цифровые платформы как вид экономических рыночных отношений и отражение этого аспекта в правовом режиме цифровых платформ // Юридические исследования. 2023. № 8. С. 96-127.

3. Законопроект № 275599-8 «О занятости населения в Российской Федерации». URL: https://sozd.duma.gov.ru/bill/275599-8

4. Количество самозанятых с начала года увеличилось в 1,2 раза до 8,06 млн. URL: https://www.interfax.ru/business/914445

5. О социальном партнерстве и разрешении трудовых споров (конфликтов): Указ Президента РСФСР №212 // Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР. 1991. № 47. Ст. 1611.

6. Платформенная занятость: вызовы и возможные решения. Центр стратегических разработок. URL: https://www.csr.ru

7. Пшеничный С. П. Инновационные элементы социального партнерства // Экономические науки. 2023. № 6. С. 435-440.

8. Пшеничный С. П. Тенденции развития института социального партнерства в России // Экономические науки. 2013. № 12. С. 47-50.

9. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ URL: https://www.consultant.ru/document/cons_doc_LAW_34683

10. YouDo запустил услугу страхования здоровья самозанятых. URL: https://news.myseldon.com/ru/news/index/246297193

А. А. Сапфирова,
доктор юридических наук, доцент,
Кубанский государственный аграрный
университет имени И. Т. Трубилина

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ В УСЛОВИЯХ ДИСТАНЦИОННОЙ РАБОТЫ

Аннотация. В статье исследуются вопросы практики применения законодательства о защите персональных данных и о дистанционном труде в их совокупности. Рассмотрены проблемы практического применения дефиниции персональных данных, запрета для отдельных работодателей обработки персональных данных в базах, не находящихся на территории РФ, и вопроса обеспечения защиты персональных данных дистанционным работником при выполнении им трудовой функции. Суть одного из выводов заключается в определении исходной точки для отнесения тех или иных сведений к персональным данным: необходимо исходить из их основного признака – возможности по этим данным идентифицировать работника. Возможным решением проблемы обеспечения дистанционным работником при выполнении трудовой функции сохранности персональных данных других работников будет закрепление в трудовом договоре территориальных запретов дистанционному работнику при осуществлении им трудовой функции.

Ключевые слова: трудовое право, дистанционный труд, персональные данные работников, трудовая функция, биометрические персональные данные, должность

PROTECTION OF PERSONAL DATA OF EMPLOYEES UNDER THE CONDITIONS OF REMOTE WORK

Abstract. The article examines the practice of applying legislation on the protection of personal data and remote work in their totality. The author considers the problems of practical application of the definition of personal data, the prohibition for certain employers of processing personal data in databases not located on the territory of the Russian Federation, and the issue of ensuring the protection of personal data by a remote worker when performing his labor function. The essence of one of the author's conclusions is to determine the starting point for classifying certain information as personal data: it is necessary to proceed from their main feature - the ability to identify an employee using this data. A possible solution to the problem of ensuring the safety of personal data of other employees by a remote worker in the performance of the labor function will be the consolidation in the employment contract of territorial prohibitions for the remote worker in the exercise of his labor function.

Keywords: labor law, remote work, personal data of employees, labor function, biometric personal data, position

Введение. В настоящее время законодательство о персональных данных и о дистанционном труде настолько часто подвергается изменениям и дополнениям, что можно утверждать, что оно полностью обновляется с учетом внедрения «цифры» в экономическую жизнь страны. Его реформирование обусловлено необходимостью обеспечить экономическую безопасность, в том числе и через защиту персональных данных работников.

Двумя годами ранее были полностью пересмотрены нормы Трудового кодекса РФ о дистанционном труде. Они позволили создать правовое поле для применения труда дистанционных работников, поскольку действовавшие до 1 января 2021 года нормы не могли надлежащим образом регулировать возникшие правоотношения с дистанционными работниками, что создавало правовой вакуум, который можно было разрешить только путем принятия новых норм о дистанционном труде.

В цифровых условиях указанные векторы совместились, что было неизбежно, и показали направления дальнейшего развития законодательства. Особое внимание законодателя к обеспечению сохранности работодателями персональных данных работников и далее будет проявляться в ужесточении ответственности за нарушение норм о защите персональных данных, что, возможно, поспособствует активности работодателей в формировании собственной локальной системы средств для информационной безопасности. И здесь речь идет не только о технических, но и о правовых средствах.

Труд дистанционных работников продолжает совершенствоваться несмотря на то, что работодатели не всегда приветствуют такую форму трудовой деятельности отчасти в связи с отсутствием у них навыков контроля труда таких работников, отчасти в связи с практическими трудностями уволить дистанционных работников, например, за прогул.

Конечно, учеными анализируются нормы о персональных данных и о дистанционном труде и практика их применения, предлагаются пути совершенствования законодательства. В их работах находим идеи, заслуживающие внимание законодателя [1–8].

В рамках настоящей статьи попытаемся, применив комплексный подход к изучению норм о персональных данных и о дистанционном труде, исследовать их применение в совокупности.

Основная часть. Во-первых, законодательство о персональных данных работников отличается разнообразием и недостаточным регулированием. Так, дефиниция «персональные данные», закрепленная в ст. 3 Федерального закона «О персональных данных» [9], не позволяет четко выразить, какие именно персональные данные являются таковыми и как определить границы тех сведений, которые можно отнести к персональным данным.

Персональные данные – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В нашей ситуации субъектом персональных данных выступает работник. Что же мы можем относить к персональным данным работника? Например, фотоизображение лица без указания его фамилии, имени, отчества [10]. В то же время если на документе указывается фамилия только с инициалами,

то идентифицировать лицо нельзя, поскольку известно, что могут встречаться не только однофамильцы, но и полные тезки [11].

Судебная практика, практика Роскомнадзора и практика работодателей разнятся в определении персональных данных. Если проанализировать их практику применения законодательства о персональных данных работников, можно сформировать перечень «неоспариваемых» персональных данных: паспортные данные, данные техпаспорта на конкретный жилой дом, данные работника из трудового договора, номер и серия паспорта; СНИЛС; ИНН; биометрические данные; счет в банке и номер карты (банковской). Хотя ИНН, например, не все суды признавали персональными данными [12], как и СНИЛС [13]. Однако это единичные случаи, которые имели место во время становления практики применения законодательства о персональных данных и, вероятно, при современном рассмотрении таких споров суды вынесли бы иные решения.

В отдельных случаях к персональным данным в их совокупности относятся: фамилия, имя, отчество, дата и место рождения, место жительства (адрес) либо фамилия, имя, отчество, должность. Возникает вопрос: относится ли номер мобильного телефона работника к его персональными данным? Положительная позиция Минцифры РФ выражается в его письме от 07.07.2017 № П11-15054-ОГ «О разъяснении норм федерального законодательства», отрицательная позиция у Роскомнадзора [14].

Думается, ответ должен быть положительным, и позиция Минцифры РФ обоснована, так как номер мобильного телефона работника – это идентификатор его личности в интернет-пространстве, позволяющий определить его как физическое лицо. Однако если номер мобильного телефона закреплен за юридическим лицом, то без связки его с конкретным работником вряд ли можно утверждать о том, что номер данного телефона – это персональные данные.

Во-вторых, вопрос о месте «дислокации» персональных данных у работодателя вызывает трудности в части защиты персональных данных.

В соответствии со ст. 18 Федерального закона «О персональных данных» [9] работодатель, собирая персональные данные работников, являющихся гражданами РФ, обязан обеспечить их обработку (например, накопление, хранение, извлечение и т. д.) с использованием баз данных, находящихся на территории РФ, за исключением случаев, указанных в данном законе (например, обработка персональных данных лиц, участвующих в гражданском судопроизводстве). Это значит, что иностранные базы данных не должны использоваться работодателями для обработки персональных данных.

Обратим внимание, что с 1 марта 2023 года установлен запрет для некоторых российских организаций использовать, в том числе для передачи персональных данных, иностранные мессенджеры, к которым отнесены, например, WhatsApp, Telegram, Viber и др. Их список можно увидеть на сайте Роскомнадзора РФ [15].

В-третьих, существует проблема обеспечения защиты персональных данных дистанционным работником при выполнении им трудовой функции.

Из анализа ст. 312.1 Трудового кодекса РФ дистанционный работник осуществляет трудовую функцию за пределами места нахождения работодателя, за

пределами стационарного рабочего места, но используя для взаимодействия с работодателем, например, Интернет или сеть связи общего пользования (например, телефон). Что из этого следует?

Это значит, что дистанционный работник может осуществлять свою трудовую функцию: 1) в любом месте мира (если только работодатель не ограничит в трудовом договоре территорию его работы), 2) в любое время (если работодатель не предусмотрит в коллективном договоре, локальном нормативном акте, трудовом договоре, дополнении к нему конкретный режим рабочего времени дистанционного работника), 3) при использовании Интернета.

Возникает вопрос: как работодатель сможет обеспечить защиту персональных данных работников своей организации, если дистанционный работник обрабатывает эти персональные данные, выполняя трудовую функцию, например, бухгалтера, рассчитывающего заработную плату? В таком случае дистанционный работник должен работать за компьютером в полностью изолированном замкнутом пространстве, причем его рабочий компьютер необходимо разместить задней частью ко входу в эту комнату, чтобы любой случайно вошедший человек не смог посмотреть информацию, с которой работает дистанционный работник. Однако у работодателя нет такой возможности проконтролировать выполнение дистанционным работником всех этих правил, что может привести к ненадлежащей защите персональных данных работников. При этом дистанционный работник может выполнять трудовую функцию, например, в парке или ином открытом пространстве (в кафе, торговом центре), работая за компьютером и обрабатывая информацию, содержащую персональные данные других работников.

Заключение. Изложенное выше дает основание для внесения предложений по практике применения законодательства о персональных данных и о дистанционном труде. Так, относя те или иные сведения к персональным данным, думается, необходимо исходить из их основного признака, а именно можно ли по этим данным определить (идентифицировать) персону (работника). Если можно, то данные следует считать персональными и в том случае, если отсутствует документ, удостоверяющий личность.

Возможным решением проблемы обеспечения дистанционным работником при выполнении трудовой функции сохранности персональных данных других работников будет закрепление в трудовом договоре территориальных запретов дистанционному работнику при осуществлении им трудовой функции.

Список литературы

1. Абдусаламов Р. А., Нурмагомедов К. М. Проблемы правовой защиты персональных данных при использовании облачных вычислений // Государственная служба и кадры. 2021. № 5. С. 20-21.

2. Сергеева Н. Ю., Шарудинова Л. Т. Защита персональных данных граждан Российской Федерации в сети Интернет: отдельные проблемы правового регулирования // Гражданин и право. 2021. № 9. С. 89-92.

3. Моллер Б. О защите персональных данных // Кадровик. 2007. № 1-3. С. 4-11.

4. Веред Е. Б. Актуальные вопросы правового регулирования труда дистанционных работников // Кадровик. 2020. № 7. С. 91-96.

5. Новикова Ю. А. Специальные категории персональных данных работников // Кадровик. 2022. № 8. С. 8-14.

6. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7-32. EDN LCCOJJ

7. Новые формы занятости в Европе / под ред. Р. Бланпэна, Ф. Хендрикса. Волтерс Клувер, 2016. 416 p.

8. Sapfirova A. A., Volkova V. V., Petrushkina A. V. Information technologies and information compliance in labor relations: legal regulation and prevention of violations of labor rights // Advances in Intelligent Systems and Computing. 2019. Vol. 726. Art. 911916.

9. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // СПС «КонсультантПлюс».

10. Постановление Президиума Верховного Суда Республики Башкортостан от 8 августа 2018 г. по делу № 44Г-300/2018 // СПС «КонсультантПлюс».

11. Апелляционное определение Верховного суда Республики Татарстан от 24 октября 2019 г. по делу № 2-5801/2019, 33-18168/2019 // СПС «КонсультантПлюс».

12. Апелляционное определение Санкт-Петербургского городского суда от 3 февраля 2015 г. по делу № 2-3097/2014 // СПС «КонсультантПлюс».

13. Решение Белоглинского районного суда Краснодарского края от 22 июня 2014 г. по делу № 2-300/2014 // СПС «КонсультантПлюс».

14. Обращения в сфере персональных данных. URL: https://15.rkn.gov.ru/p8880/p15987/

15. Вниманию российских организаций, использующих иностранные сервисы. URL: https://rkn.gov.ru/news/rsoc/news74672.htm

К. Л. Томашевский,
доктор юридических наук, профессор,
Казанский инновационный университет
имени В. Г. Тимирясова

ЭЛЕКТРОННЫЙ КАДРОВЫЙ ДОКУМЕНТООБОРОТ: НОВОВВЕДЕНИЯ В ТРУДОВОМ ЗАКОНОДАТЕЛЬСТВЕ БЕЛАРУСИ И ИХ СРАВНЕНИЕ С ОПЫТОМ РОССИИ

Аннотация. В статье проведен анализ нововведений в части регламентации электронного кадрового документооборота в Республике Беларусь, в особенности ст. 29^1 «Совершение сторонами трудовых отношений действий в электронном виде», которая вводится в Трудовой кодекс Беларуси с 01.01.2024. Проводится сравнительный анализ этих нововведений с правилами электронного кадрового документооборота, ране введенными в Трудовой кодекс Российской Федерации. Высказываются предложения по гармонизации норм трудового законодательства Беларуси и России по вопросам электронного кадрового документооборота при приеме на работу и в процессе трудовой деятельности работника.

Ключевые слова: право, цифровизация, электронный кадровый документооборот, работодатель, наниматель, работник, трудовой договор, трудовые отношения

ELECTRONIC PERSONNEL DOCUMENT MANAGEMENT: INNOVATION IN THE EMPLOYMENT LEGISLATION OF BELARUS AND COMPARATIVE ANALYSIS WITH EXPERIENCE OF RUSSIA

Abstract. The paper analyzes the innovations regarding the regulation of electronic personnel document management in the Republic of Belarus, especially article Art. 29[1] «The parties to perform labor relations in electronic form», which is introduced into the Labor Code of Belarus from 01.01.2024. A comparative analysis of these innovations is carried out with the rules of electronic personnel document management introduced in the Labor Code of the Russian Federation. Suggestions are made on the harmonization of labor legislation in Belarus and Russia on issues of electronic personnel document management when applying for a job and in the process of the employee's labor activity.

Keywords: law, digitalization, electronic personnel document management, employer, employee, employment contract, employment relations

В условиях расширения внедрения цифровых технологий во все сферы жизни современного общества особое значение они приобретают как на стадии приема на работу, так и в процессе существования трудовых отношений. В статье коснемся нововведений в регулировании электронного взаимодействия между работником и нанимателем (работодателем) в Беларуси с учетом предшествующего опыта России.

Законом Республики Беларусь от 29.06.2023 № 273-З «Об изменении законов по вопросам трудовых отношений» Трудовой кодекс Республики Беларусь (далее – ТК РБ) дополнен новой ст. 29[1] «Совершение сторонами трудовых отношений действий в электронном виде», которая вступит в силу с 01.01.2024.

Согласно ст. 29[1] ТК РБ, предупреждение работника, получение от него согласия, ознакомление, в том числе под роспись, с локальными правовыми актами (далее – ЛПА или ЛНА), приказами (распоряжениями) нанимателя, уведомлениями, требованиями и иными документами, ведение которых предусмотрено законодательством о труде, а также обращение работника к нанимателю и иные действия, предусмотренные ТК РБ, кроме заключения, продления и изменения трудовых договоров, договоров о полной материальной ответственности, могут совершаться в электронном виде при условии, что программно-технические средства, используемые нанимателем, позволяют однозначно идентифицировать работника, а также с использованием электронной цифровой подписи. Решение о совершении действий, указанных в ч. 1 данной статьи, в электронном виде и порядок их совершения устанавливаются ЛПА.

Обратим внимание, что двумя годами ранее более детализированные нормы об электронном взаимодействии работника, а также лица, поступающего на работу с одной стороны и работодателя с другой стороны были включены в виде трех новых статей (ст. 22.1–22.3) в Трудовой кодекс Российской Федерации (далее – ТК РФ). Речь идет о Федеральном законе от 22.11.2021 № 377-ФЗ «О внесе-

нии изменений в Трудовой кодекс Российской Федерации». Большинство изменений, внесенных этим законом, действуют с конца 2021 г., но требования к составу и форматам электронных документов стали применяться с 01.03.2023. Детальный научный анализ законопроекта и судебной практики использования электронного кадрового документооборота представлен в статье С. Ю. Головиной и Л. В. Зайцевой [1]. Попытки откомментировать вышеуказанные новые нормы ТК РФ уже предпринимались российскими авторами [2]. В Беларуси подготовлен комментарий к последним изменениям в ТК РБ, включая новую ст. 29^1 [3].

Появление соответствующих статей в ТК РФ (ст. 22.1–22.3) и включение ст. 29^1 в ТК РБ связано с развитием цифровой экономики, широкомасштабными процессами цифровизации, в том числе с внедрением цифровых технологий в трудовые отношения, а электронного документооборота в кадровое делопроизводство.

Введение вышеуказанных норм в трудовое законодательство России и Беларуси обусловлено целями предоставления возможности использования в трудовых отношениях аналогов собственноручной подписи (электронной цифровой подписи и ее разновидностей) наряду с собственноручной подписью. Решение законодателей представляется концептуально верным, поскольку в условиях повсеместной цифровизации трудовых отношений электронный формат взаимодействия сторон трудового договора постепенно вытесняет письменный (бумажные носители).

Вместе с тем помещение ст. 29^1 в гл. 2 ТК РБ «Заключение трудового договора» представляется, на наш взгляд, нелогичным. Правильнее было бы расположить эти нормы в гл. 1 «Общие положения», поскольку речь идет об ознакомлении с ЛПА, приказами, распоряжениями нанимателя, уведомлениями (последние, к примеру, могут быть использованы не столько при заключении трудового договора, сколько при изменении и прекращении трудового договора, при предоставлении трудовых и социальных отпусков и т. д.) [4. С. 76], то есть эти нормы носят сквозное значение для различных институтов особенной части трудового права. В этом плане более логичное решение было принято российским законодателем, поместившим правила об электронном кадровом документообороте в сфере труда в разделе I ТК РФ «Общие положения».

Правило ч. 1 ст. 29^1 ТК РБ распространяется не только на приказы и распоряжения, но также и на другие организационно-распорядительные документы нанимателя, в том числе постановления, решения, а также на акты, протоколы, отчеты и другие, учитывая неисчерпывающий перечень документов («и иными документами»).

В ч. 1 ст. 29^1 ТК РБ содержится открытый перечень действий сторон трудового договора, которые могут быть совершены в электронном виде, а именно:

– предупреждение работника (например, о предстоящем увольнении работника по п. 1 и 2 ст. 42 согласно ч. 3 ст. 43);

получение от работника согласия (в частности, согласия на привлечение к сверхурочной работе по ч. 1 ст. 120, к работе в выходной день согласно ч. 1 ст. 142 и т. п.);

– ознакомление, в том числе под роспись, с ЛПА (облегчается выполнение нанимателем обязанностей, предусмотренных п. 2 и 3 ч. 1 ст. 54, п. 10 ч. 1 ст. 55,

в частности по ознакомлению работника с коллективным договором, ПВТР, должностной или рабочей инструкциями, положениями о структурном подразделении, иными ЛПА, с изменениями и дополнениями к ним);

– ознакомление, в том числе под роспись, с приказами (распоряжениями) нанимателя, уведомлениями, требованиями и иными документами, ведение которых предусмотрено законодательством о труде (к примеру, речь может идти об ознакомлении с приказами об установлении совмещения должностей служащих, профессий рабочих, расширении зон обслуживания (увеличении объема работы), исполнении обязанностей временно отсутствующего работника, о предоставлении трудовых и социальных отпусков, направлении в служебные командировки, на повышение квалификации, осуществлении гарантийных или компенсационных выплат, премировании, депремировании, поощрении, наложении дисциплинарных взысканий, удержаниях из заработной платы, проведении аттестации работников и т. д.);

– обращение работника к нанимателю (подача заявлений об увольнении, о предоставлении трудового отпуска, социального отпуска, о выплате денежной компенсации вместо части трудового отпуска, об обеспечении средствами индивидуальной защиты, подача объяснительной записки в отношении дисциплинарного проступка и т. п.);

– иные действия, предусмотренные ТК РБ (к этим иным действиям могут быть отнесены, к примеру, уведомления профсоюза о предстоящем увольнении работника по некоторым основаниям, связанным с инициативой нанимателя, согласно ч. 1 и 2 ст. 46, сообщение собственнику или уполномоченному им органу, поставщикам, потребителям, транспортным организациям, местному исполнительному и распорядительному органу о предстоящей забастовке согласно ч. 2 ст. 390).

Для сравнения: российский законодатель в правилах ст. 22.1–22.3 ТК РФ не дает подробного перечня случаев взаимодействия работодателя с работником или лицом, устраивающимся на работу, с комиссией по трудовым спорам, поскольку дать исчерпывающий перечень этих ситуаций не представляется возможным, а давать открытый (неисчерпывающий) вряд ли нужно.

Как белорусский, так и российский законодатели оговаривают исключения, в отношении которых электронный документооборот и электронная форма взаимодействия не могут применяться. Так, в ч. 1 ст. 29^1 ТК РБ сделана оговорка «кроме заключения, продления и изменения трудовых договоров, договоров о полной материальной ответственности». Это исключение означает, что действия работника или нанимателя, связанные с заключением трудового договора (заявление о приеме на работу, ознакомление с приказом о приеме на работу), продлением контракта (взаимное письменное предупреждение нанимателем и работником друг друга о решении продолжить или прекратить трудовые отношения согласно п. 6 и п. 7 ч. 1 ст. 261^2 и ч. 2 ст. 261^3), изменением трудового договора (заявление с просьбой о постоянном переводе согласно ч. 2 ст. 30, выражение согласия на временный перевод сроком до 6 месяцев в течение календарного года согласно п. 1 ч. 1 ст. 32^1, письменное предупреждение нанимателем работника об изменении существенных условий труда согласно ч. 3 ст. 32) должны совершаться только

в письменной форме. Это же исключение из общего правила распространяется на заключение договора о полной индивидуальной материальной ответственности (ст. 405) и полной коллективной (бригадной) материальной ответственности (ст. 406), которые могут совершаться только в письменной форме. Вместе с тем, учитывая правило ч. 1 ст. 22 Закона Республики Беларусь от 28.12.2009 № 113-З «Об электронном документе и электронной цифровой подписи», согласно которому электронный документ приравнивается к документу на бумажном носителе, подписанному собственноручно, и имеет одинаковую с ним юридическую силу, при наличии ЭЦП как у нанимателя, так и у работника полагаем, что использование электронного документа в перечисленных выше случаях также вполне допустимо с позиции действующего законодательства.

Как российский, так и белорусский законодатели предусмотрели локальный уровень правового регулирования электронной формы взаимодействия сторон трудового договора. Следовательно, для использования электронного кадрового документооборота, заменяющего собой письменный, работодатель (наниматель) должен разработать и принять соответствующий ЛНА, с которым должны быть ознакомлены все работники организации. Причем данный ЛНА (согласно ТК РФ) принимается работодателем с учетом мнения выборного органа первичной профсоюзной организации в порядке, установленном ст. 372 ТК РФ, для принятия ЛНА (по ст. 29^1 ТК РБ соблюдения этой процедуры не требуется). В ч. 2 ст. 22.2 ТК РФ установлены более четкие требования (в сравнении с ТК РБ) к содержанию ЛПА по вопросам электронного кадрового документооборота. Полагаем, что эти нормы из ТК РФ могут быть в последующем учтены и даже позаимствованы белорусским законодателем при совершенствовании ст. 29^1 ТК РБ.

В заключение отметим, что российский законодатель в Федеральном законе от 22.11.2021 № 377-ФЗ «О внесении изменений в Трудовой кодекс Российской Федерации» легально увязал использование работниками и работодателями цифровой платформы «Работа в России» и единого портала государственных и муниципальных услуг (Госуслуги) с электронными инструментами электронного кадрового документооборота, используемыми работодателем. Это концептуально правильное решение позволяет существенно облегчить взаимодействие работодателя с различными органами власти и управления, создавая прозрачную цифровую среду, в которой обеспечивается доступ к персональным данным работников со стороны Социального фонда России (с 01.01.2023 он объединил в себе ПФР и ФСС), государственной службы занятости, учреждений обязательного медицинского страхования и т. д. Этот позитивный опыт также может представлять интерес для нормотворческих органов Республики Беларусь.

Список литературы

1. Головина С. Ю., Зайцева Л. В. Электронный кадровый документооборот: от правового эксперимента к практике // Правоприменение. 2022. № 6(2). С. 241-256.

2. Комментарий к Трудовому кодексу Российской Федерации (постатейный). 6-е изд. / О. А. Шевченко, Ф. О. Сулейманова, Г. В. Шония, С. Н. Кудряшова; под ред. Шевченко О. А. М.: Проспект, 2023.

3. Комментарий изменений и нововведений в Трудовой кодекс Республики Беларусь (с учетом изменений, вступающих в силу 1 января 2024 года) / Н. А. Адашкевич, Е. А. Волк [и др.]; под общ. ред. Л. И. Липень, Б. Б. Синькова. Минск: Амалфея, 2023.

4. Томашевский К. Л. Изменения в Трудовом кодексе: расширение возможностей использования электронного документооборота, новые гарантии // Отдел кадров. 2022. № 3. С. 76-80.

М. С. Чистяков,
младший научный сотрудник,
Российский университет кооперации,
Владимирский филиал
Е. В. Кирова,
старший преподаватель,
Российский университет кооперации,
Владимирский филиал
Д. И. Лукашина,
преподаватель,
Финансовый университет
при Правительстве Российской Федерации,
Владимирский филиал

О ВАРИАТИВНОСТИ ПЕРЕХОДНОГО ЭТАПА ВЕДЕНИЯ ТРУДОВОЙ КНИЖКИ

Аннотация. Рассматривается вариативность ведения трудовой книжки в лиминальный период перехода на электронный документооборот кадрового документооборота. Приводится краткая историческая хронология возникновения трудовой книжки, ее преобразования в процессе становления трудового законодательства и развития структуры кадровой службы предприятий. Эпоха «Индустрии 4.0» позиционируется в качестве основы специфических черт электронного кадрового документооборота. Рассматриваются при этом аргументы сторонников и противников цифровой формы фиксирования трудовой истории.

Ключевые слова: трудовая книжка, кадровый документооборот, «Индустрия 4.0», трудовая история, кадровые службы, трудовое законодательство, цифровая экосистема, электронная форма

ON THE VARIABILITY OF THE TRANSITION STAGE MAINTAINING A WORK RECORD

Abstract. The variability of maintaining a work record book in the liminal period of transition to electronic document management of personnel document management is considered. A brief historical chronology of the appearance of the work book, its transformation in the process of formation of labor legislation and the development of the

structure of the personnel service of enterprises is given. The authors of the publication position the era of «Industry 4.0» as the basis of specific features of electronic personnel document management, while considering the arguments of supporters and opponents of the digital form of recording labor history.

Keywords: employment record, personnel document management, «Industry 4.0», labor history, personnel services, labor legislation, digital ecosystem, electronic form

Процедура ведения кадрового документооборота имеет принципиально важное значение на протяжении всей трудовой и последующей жизни каждого человека. Отдельного внимания, по мнению представителей экспертного сообщества, заслуживает ведение трудовых книжек (далее – ТК) – как в привычном бумажном варианте, так и в электронной форме (далее – ЭТК).

Привычная российскому обывателю ТК существует более ста лет. Первое упоминание о кадровом документе зафиксировано в Декрете Совета Народных Комиссаров 1918 года «О трудовых книжках для нетрудящихся» [3]. Обязанность иметь ТК всем трудящимся была закреплена также в Кодексе законов о труде РСФСР 1918 года. В данном варианте ТК просуществовали сравнительно недолго. С 15 ноября 1922 года данный документ заменяется расчетными книжками (Кодекс законов о труде РСФСР 1922 года). 21 сентября 1926 г. в историографии кадрового документа известен вводом в оборот трудовых списков, отражающих трудовую активность населения. В трудовых списках работодатель обязан был отражать дату приема на работу, должность работника, получаемую заработную плату и иную информацию, связанную с выполняемыми должностными обязанностями. Данный документ имел схожие черты с формулярными списками, существовавшими до 1917 года [2. С. 221]. В 1939 году в Советском Союзе в оборот вводится ТК, обязательная для всех трудящихся учреждений и предприятий [4].

Тенденции эпохи «Индустрии 4.0» привнесли изменения и в работу кадровых служб, в которой все больше информации фиксируется в «цифре», заменяя привычный формат бумажного делопроизводства. Отметим, что зарубежный опыт электронного кадрового документооборота значительно опережает отечественное кадровое делопроизводство. В США и ЕС электронный оборот кадровых документов был введен в начале 2000-х годов. Россия только приступила к реализации концепции перевода в «цифру» кадровых документов, при этом основными акторами в данном процессе являются крупные предприятия.

Процесс ведения ТК в цифровой форме позволяет сформировать концепцию генерации единой информационной платформы кадрового документооборота, обладающего значительным массивом персонифицированной информации, о чем свидетельствует проект перевода в «цифру» кадровых документов 60 млн трудящихся на 8,5 хозяйствующих субъектов [1].

Гибкость регулирования трудовых взаимоотношений, к которым относится электронный кадровый документооборот (далее – ЭКД), применение цифровых платформ и сервисных технологий, снижает бюрократические препоны для развития малого и среднего предпринимательства, является одним из элементов перехода с традиционных методов управления экономикой к цифровым.

Пояснительная записка к проекту данного законодательного акта зафиксировала целеполагание перехода на ЭКД: обеспечительные меры сохранности сведений о трудовой деятельности; снижение затрат работодателя при производственных мероприятиях кадрового документооборота; упрощение взаимодействия между работником, работодателем и государственными структурами, в компетенции которых входит сбор, анализ и хранение информации о трудовой деятельности граждан [9].

У граждан, сохранивших действующую ТК в бумажном варианте, остается возможность перейти на электронный вариант, в отличие от сотрудников, уже перешедших на данную форму (пункт 5 статьи 2 Федерального закона от 16.12.2019 № 439-ФЗ [8]. Переход обратно на бумажный носитель законодатель не предусматривает.

Для популяризации ведения ТК в электронной форме необходима соответствующая разъяснительная работа и создание референтной транспарентной экосистемы кадрового документооборота. Преобразования предполагают правовую эквивалентность ТК в электронном формате и привычном (бумажном) носителе [12. С. 95].

Приведем отличительные характерные признаки бумажного и электронного формата ТК [7].

Специфические критерии вариаций ведения трудовой книжки

Описываемый критерий	**Документ на бумажном носителе**	**Электронный документ**
Внесение записей в трудовую книжку	Заполняется собственноручно чернилами специалистом кадровой службы	Заполнение производится при использовании специального программного обеспечения
Отображение занесенной информации	В бумажной форме ТК	В электронном виде без привязки к физическому носителю (в виде привычной бумажной ТК)
Привязка процесса автоматизации фиксирования кадровых мероприятий	Нереализуем	Реализуем посредством ряда операций (сканирование, автозаполнение, распознавание вносимой информации)
Транспарентность	Отсутствует	Возможна

Сторонники ЭТК в качестве одного из преимуществ электронного формата приводят отсутствие возможности у недобросовестного работодателя удерживать ТК при увольнении сотрудника. Хотя действующее трудовое законодательство обязывает представителя нанимателя выдать ТК в день прекращения трудовой деятельности, нередки случаи задержки документа под различными предлогами. Особенно данный вариант распространен при наличии многочисленных филиалов у крупного предприятия или при дистанционной работе. Напротив, работник, выбравший электронную форму ТК, становится более мобильным в выборе вариантов трудоустройства [11]. Использование ЭТК на соответствующих цифровых платформах упрощает нивелирование ошибок и минимизирует человеческий фактор, что снижает вероятность технических неточностей и опечаток при занесении в кадровые документы информации. Кроме того, электронный документооборот

послужит катализатором развития цифровых технологий и генерации особой цифровой экосистемы предприятия.

Явный приоритет выбора ЭТК прослеживается при дистанционной (удаленной) занятости, поскольку часто взаимоотношение работника и кадровой службы предприятия осуществляется посредством цифровых технологий (электронной переписки, видео-, мобильной связи и т. д.) [5].

ЭКД позволит в режиме онлайн осуществлять:

– мониторинг численности работающих – как в отдельном хозяйствующем субъекте, так и в более крупных масштабах (города, региона, округа);

– аналитическую работу и обработку данных в целях оперативного мониторинга состояния рынка труда; соотношения численности занятых и безработных среди трудоспособного населения, в том числе в контексте дифференцированных характеристик (пол, возраст, профессия, уровень образования, стаж и т. д.);

– прогнозировать динамику востребованных профессий, планировать и корректировать численность подготавливаемых специалистов по данным видам специальностей.

ЭКД в конвергенции с межведомственным взаимодействием способствует условиям упрощенного оформления социальных выплат, включая пенсионное обеспечение.

Тем не менее противники электронной «кадровой истории» аргументируют свою позицию вероятностью утечки персонифицированной информации, которая в руках злоумышленников становится орудием корыстных манипуляций и мошеннических действий [10], что, в условиях стремительного развития цифровых технологий и транспарентности для них государственных границ, барьеров заградительного трансфера – снижает доверие обычного обывателя к данной вариации кадрового документооборота.

Остается актуальным вопрос ущемления прав граждан, впервые трудоустраивающихся с 2021 года, так как им не оставляют выбора формы ведения трудовой истории. Данной категории сведения о трудовой деятельности формируются в электронном виде. Тем самым нарушается принцип равенства работников, их прав и возможностей, зафиксированных в ст. 2 Трудового кодекса Российской Федерации [6].

Отметим наличие дополнительной нагрузки на кадровые службы предприятий при параллельном ведении бумажного носителя и электронной формы ТК, а также значительный объем работы по формированию сведений о трудовой деятельности всех работников, выбравших ЭТК, возложенный на подразделения управления персоналом.

Устоявшаяся в последнее время в общественном сознании формулировка «электронная трудовая книжка» – не что иное, как метафора, представляющая собой вариативный формат фиксации, отражения и хранения информации о трудовой деятельности человека. Трансформация кадрового документооборота, учитывая глобальную цифровизацию социума, представляет собой стратегическую необходимость формирования цифровой среды, что коррелирует с национальной программой «Цифровая экономика России».

Список литературы

1. В 2021 году все бумажные трудовые книжки вернут работникам. URL: https://rg.ru/2019/07/09/v-2021-godu-vse-bumazhnye-trudovye-knizhki-vernut-rabotnikam.html

2. Губанова О. А. Трудовые книжки в России с 1917 года до наших дней: материалы Международной научно-практической конференции «Подготовка кадров в системе предупреждения и ликвидации последствий чрезвычайных ситуаций». СПб.: Санкт-Петерб. ун-т Государственной противопожарной службы, 2018. С. 221-225.

3. Декрет Совета Народных Комиссаров РСФСР «О трудовых книжках для нетрудящихся» от 10.05.1918 // Собрание узаконений и распоряжений правительства за 1917–1918 гг. Управление делами Совнаркома СССР. М., 1942. С. 1003-1006.

4. Постановление СНК СССР «О введении трудовых книжке» от 21.12.1938 № 1320. URL: https://normativ.kontur.ru/document?moduleId=1&documentId=286865

5. Практические рекомендации по удаленке: на что обратить внимание кадровику. URL: https://www.kdelo.ru/art/386297-prakticheskie-rekomendatsii-po-udalnke-na-chto-obratit-vnimanie-kadroviku

6. Статья 2 ТК РФ (последняя редакция с комментариями). Основные принципы правового регулирования трудовых отношений и иных непосредственно связанных с ними отношений. URL: https://www.trudkod.ru/chast-1/razdel-1/glava-1/st-2-tk-rf#:~:text=%

7. Трудовая книжка в электронном виде в 2023 году. URL: https://pravo-invalida.ru/elektronnye-trudovye-knizhki/

8. Федеральный закон «О внесении изменений в Трудовой кодекс Российской Федерации в части формирования сведений о трудовой деятельности в электронном виде» от 16.12.2019 № 439-ФЗ // Собрание законодательства РФ. 2019. № 51. Ст. 7491.

9. Финансово-экономическое обоснование к проекту Федерального закона «О внесении изменений в Трудовой кодекс Российской Федерации (в части формирования сведений о трудовой деятельности в электронном виде)». URL: https://sozd.duma.gov.ru/bill/1162885-7?ysclid=lm7hdb2yx5264223481

10. Чирков М. А., Золкин А. Л., Чистяков М. С., Лукашина Д. И. Социальная инженерия как фактор способствования мошенническим действиям в цифровой среде // Философия хозяйства. 2021. № 4(135). С. 216-229.

11. Чистяков М. С. Ликвидация трудовой книжки как фактор трансформационных изменений трудовых отношений // Материалы VIII Международной научной конференции «Экономика, управление, финансы». Краснодар: Новация, 2018. С. 125-130.

12. Шумилина М. А., Нефедова К. А., Чистяков М. С. «Индустрия 4.0» как инструмент кадрового менеджмента в реализации кадрового документооборота: материалы I Всероссийской научно-практической конференции молодых ученых «Актуальные проблемы развития экономики, права, кооперации». Уфа: Изд-во Башкирского кооперативного института, 2021. С. 94-97.

Ю. О. Шишкина,
старший преподаватель,
Сибирский институт бизнеса и информационных технологий

СМАРТ-КОНТРАКТ И БЛОКЧЕЙН В РЕГУЛИРОВАНИИ ТРУДОВЫХ ОТНОШЕНИЙ В РОССИИ: ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ РАЗВИТИЯ

Аннотация. В статье рассматриваются такие понятия как смарт-контракт, блокчейн. Устанавливаются преимущества и недостатки для работников и работодателей перехода к данной системе. Анализируются нормативные правовые акты, регулирующие вышеуказанные правоотношения. В заключение приводится вывод, что блокчейн и смарт-контракт в настоящее время не урегулированы законодательством Российской Федерации. Возникает много вопросов с применением вышеуказанных способов при регулировании трудовых отношений.

Ключевые слова: смарт-контракт, блокчейн, электронная цифровая подпись, работник, работодатель

SMART CONTRACT AND BLOCKCHAIN IN THE REGULATION OF LABOR RELATIONS IN RUSSIA: FEATURES AND PROSPECTS OF DEVELOPMENT

Abstract. This article discusses concepts such as smart contract, blockchain. The advantages and disadvantages for employees and employers of the transition to this system are established. The normative legal acts regulating the above-mentioned legal relations are analyzed. In conclusion, the author comes to the conclusion that blockchain and smart contract are currently not regulated by the legislation of the Russian Federation. There are many questions with the use of the above methods in the regulation of labor relations.

Keywords: smart contract, blockchain, electronic digital signature, employee, employer.

Введение. В настоящее время происходит развитие и цифровизация экономики и других отраслей жизни общества. Появление искусственного интеллекта диктует свои правила, и отрасли права, в том числе трудовое законодательство, подстраиваются под эти изменения. Претерпевают изменения нормы, регулирующие трудовые отношения.

Дистанционный труд, по сути, и был первым шагом в процессе трансформации трудовых отношений. В настоящее время требуется пересмотреть саму систему трудоустройства, оформления трудовых отношений и иные моменты, связанные с цифровизацией общества

Основная часть. С появлением пандемии COVID-19 жизнь изменилась во всех сферах, не стали исключением и трудовые отношения. Дистанционная работа, которая раньше была распространена на отдельную категорию работников стала, по сути, обязательной для всех. В период распространения коронавирусной

инфекции стали внедряться технологии онлайн-трансляций, раннее не использовавшиеся массово в трудовых отношениях.

В сложившейся ситуации стали применять различные цифровые технологии и различные подходы, упрощающие поиск информации, а также вводиться новые технологии для удобства обмена информацией и взаимодействия работника и работодателя.

Так, до пандемии в пп. «г» п. 41 Указа Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» было прописано, что основными задачами применения информационных технологий в сфере взаимодействия государства и бизнеса, формирования новой технологической основы в экономике являются:

г) продвижение проектов по внедрению электронного документооборота в организациях, создание условий для повышения доверия к электронным документам, осуществление в электронной форме идентификации и аутентификации участников правоотношений [6].

И в п. 4.1. «Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации»» [3] указывалось, что также концептуальные акты будут направлены на совершенствование и гармонизацию законодательства в целях удовлетворения потребностей цифровой экономики, разработку принципов и подходов к трансграничному регулированию отношений в цифровой среде, подготовку предложений по комплексному правовому регулированию применения новых технологий, внедрение механизмов сбора сведений о международном опыте регулирования отношений в сфере цифровой экономики.

При всех принятых вышеуказанных актах и вступивших в силу изменениях в Гражданский кодекс РФ нигде не содержится понятий «смарт-контракт» и «блокчейн».

Разберем данные понятия.

Так, А. И. Савельев под смарт-контрактом понимает договор, существующий в форме программного кода, имплементированного на платформе блокчейн, который обеспечивает автономность и самоисполнимость условий такого договора по наступлении заранее определенных в нем обстоятельств [5. С. 32–60].

По мнению Л. А. Новоселовой, «блокчейн – это компьютерная технология, построенная на особой системе шифрования, т. е. по сути дела, информационная база, которая строится по принципу добавления блоков» [2].

На сегодняшний день пошла такая тенденция, что работники стараются перейти на удаленную работу или их переводят работодатели в целях экономии арендной платы или в иных случаях, а также просто отказ работодателя от наемного труда и замена работников роботами.

Данный факт в скором времени может полностью заменить людей в определенных секторах экономики, соответственно, работодатели могут отказаться полностью или частично от определенной категории работников, что может привести к безработице.

Данное явление уже прослеживается среди следующей категории работников:

– кондукторов, которых частично заменили валидаторами;

– кассиров, которых заменили кассами самообслуживания;

– доставщиков (практика есть в Москве), где еду доставляет робот и некоторые другие категории работников.

В данных условиях следует внести изменения в отдельные нормы трудового права, актуализировать действующее законодательство в эпоху современного прогресса. Помимо этого, понадобится регламентировать (в тех случаях, когда труд совместный, а именно компьютера и человека) отдельные нормы охраны труда, потому что у одного работодателя могут работать и робот, и работник. Также работодателю, который наравне с работником использует робота, нужно быть готовым к его поломкам и, соответственно, к своевременному обслуживанию и осматриванию данной техники.

Так, Пенсионный фонд России 29 августа 2018 года опубликовал следующую информацию: «Внедрение смарт-контрактов в трудовые отношения позволит в будущем отказаться от обязательного заключения их в бумажном виде, но иметь о них информацию в любой момент времени, как это сегодня происходит с правом на недвижимость» [4].

Кроме того, ПФР планирует использовать в своей работе технологию блокчейн, которая «позволит распределить информацию о трудовых договорах между работодателями и удостоверяющими центрами». Это защитит граждан от нерадивых работодателей, которые оформляют трудовые договоры с нарушением законодательства [4].

Преимущество использования блокчейна для хранения информации о трудовых контрактах в том, что внесение правок в документы задним числом станет невозможным. На данный момент сведения о налоговых отчислениях и страховых взносах работодателей хранятся на серверах ведомства» [4].

У данной эффективной возможности применения блокчейна и использования его в трудовых отношениях есть две стороны медали, как для работника, так и для работодателя.

Обратим внимание на недостатки для работодателей. Для них естественный минус затратности. Во-первых, стоимость электронной цифровой подписи. Не все организации могут позволить себе ее приобрести. Во-вторых, проблемы защиты от кражи электронной цифровой подписи. В настоящий момент участились кражи электронной цифровой подписи и стопроцентных гарантий защиты подписи не существует. В-третьих, не всегда работодатель хочет законно трудоустраивать работников. В-четвертых, как и любая цифровая система, данная система может дать сбой и информация о выплатах, оформленных трудовых договорах и другие данные будут потеряны или окажутся у третьих лиц. Введенная система должна обладать надежной защитой от атак хакеров, а также не попасть в руки к конкурентам. Такая защита достаточно дорогостоящая и не все предприятия и организации смогут себе ее позволить. В-пятых, во избежание утраты данных и наказания виновных могут внести соответствующие изменения в КоАП РФ или УК РФ о привлечении работодателя или ответственного работника за сохранность данной системы к административной или уголовной ответственности за несохранение

данных работников (в случае их утраты или перехода к третьим лицам), ненадлежащую защиту системы или несвоевременное реагирование при хакерских атаках. Такие минусы не будут способствовать тому, что работодатели массово будут внедрять в свои организации блокчейн.

Единственное преимущество для работодателя в данной ситуации – это уменьшение бумажной работы, уменьшение архивов и баз данных работников.

Недостатки для работников. Во-первых, риск потери данных без возможности восстановления. Во-вторых, невозможность работать за зарплату в конверте. В-третьих, уменьшение числа сотрудников на предприятии ввиду электронного документооборота. В-четвертых, вероятность снижения заработной платы ввиду затратности данной системы.

Преимущества для работников. Во-первых, официальное трудоустройство. Во-вторых, быстрая передача информации и всех данных о работнике. В-третьих, быстрое заключение, изменение и расторжение трудовых договоров.

Стив Хамм (Steve Hamm) утверждает, что «блокчейн, основанный на «умных» контрактах, сможет привести к значительным изменениям в отдельных отраслях, к появлению новых бизнес-моделей» [1. С. 37–47].

С данным утверждением нельзя не согласиться, но применять данные технологии нужно тогда, когда соответствующая отрасль к ним готова и может измениться под них.

Заключение. Цифровые технологии применяются широко на практике, но трудовые отношения достаточно специфичны и поэтому требуют особенных и проработанных способов внедрения, регулирования, изменения, контроля, ответственности перехода к вышеуказанной системе. В трудовом праве пока не выработана методика взаимодействия в данной системе, также нет гарантий утраты данных о работниках без возможности их восстановления. На данный момент массовое использование данной технологии невозможно ввиду отсутствия того уровня гарантий и защиты баз данных, при которых можно было бы говорить о стандартизации и повсеместном введении этой системы.

Список литературы

1. Гумеров Э. А., Алексеева Т. В. Особенности технического задания на разработку блокчейн-систем управления // Прикладная информатика. 2020. Т. 15, № 2(86). С. 37-47.

2. Ермакова И. В. Влияние сетевизации экономики на изменение положений конкурентного права (на примере блокчейн и смарт-контрактов в области рекламы и права интеллектуальной собственности) // Юридические исследования. 2020. № 9.

3. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации»: Утвержден президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7. URL: https://www.consultant.ru/document/cons_doc_LAW_328854/

4. Пенсионный фонд России перейдет на блокчейн. URL: https://www.sostav.ru/publication/pensionnyj-fond-rossii-perejdyot-na-blokchejn-33060.html

5. Савельев А. И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. 2016. № 3. С. 32-60.
6. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

С. В. Шуралева,
кандидат юридических наук, доцент,
Пермский государственный
национальный исследовательский университет

УЯЗВИМЫЕ ГРУППЫ РАБОТНИКОВ В ЭПОХУ МАШИН: РИСКИ И ПЕРСПЕКТИВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ

Аннотация. Работа посвящена исследованию рисков для уязвимых групп работников в связи с внедрением искусственного интеллекта и автоматизации рабочих мест. Рассмотрение категории уязвимости через призму экономических и социологических подходов позволяет автору констатировать, что социологическая концепция социального исключения наиболее близка к юридическому пониманию уязвимости. На основе анализа возможных рисков внедрения автоматизации и искусственного интеллекта для уязвимых групп работников предложены перспективные направления модернизации трудового законодательства.

Ключевые слова: автоматизация, алгоритмы, искусственный интеллект, концепция социального исключения, дискриминация, уязвимые группы работников, цифровые технологии

VULNERABLE GROUPS OF EMPLOYEES IN THE AGE OF MACHINES: RISKS AND PROSPECTS OF LEGAL REGULATION

Abstract. The article studies risks for vulnerable groups of employees in connection with the artificial intelligence and automation. Considering the vulnerability through the prism of economic and sociological approaches allows the author to state that the sociological concept of social exclusion is closest to the legal understanding of vulnerability. Based on the analysis of possible risks of the introduction of automation and artificial intelligence for vulnerable groups of employees, directions for improving labor legislation are proposed.

Keywords: automation, algorithms, artificial intelligence, the concept of social exclusion, discrimination, vulnerable groups of employees, digital technologies

Введение. Сквозные цифровые технологии уже оказали огромное влияние на нашу жизнь и продолжат существенно трансформировать ее в ближайшие десятилетия. Так, например, технологии искусственного интеллекта (далее – ИИ) обеспечивают людям все больший комфорт потребления: рекомендательные системы помогут сделать выбор среди огромного количества товаров, голосовой

помощник способен разобраться с домашними делами и даже развлечь ребенка, чат-бот первым придет на помощь, если возникли проблемы на Госуслугах или в мобильном приложении банка.

Неудивительно, что фокус современных экономических исследований направлен в основном на человека-потребителя, а не на человека-работника, несмотря на то, что работа по-прежнему занимает значительную часть жизни и служит большинству людей источником средств для потребления.

«Обесценивание» работы нивелирует серьезную проблему влияния автоматизации и ИИ на труд и занятость людей, работающих по найму, в особенности – на уязвимые группы работников.

Основная часть. Понимание уязвимости во многом предопределяется используемыми научными подходами. Концепция бедности в рамках экономической теории использует монетарный и немонетарный подходы. Они отличаются инструментами измерения бедности. В монетарном подходе для этого используются показатели душевых доходов населения и прожиточный минимум. Немонетарный подход учитывает индексы возможностей и лишений, определяющие несоответствие уровня потребления отдельных домохозяйств принятому в обществе стандарту, отсутствие доступа к определенному набору благ [6. С. 33], т. е. использует более обширный перечень показателей.

Преимуществом рассмотрения уязвимости как состояния бедности является относительная простота и удобство инструментария измерения. Однако прожиточный минимум или общественный стандарт потребления может быть искусственно занижен. Кроме того, очевидно, что причиной уязвимости может быть не только неудовлетворительное имущественное положение. Однако «именно монетарный подход вследствие четкости критериев и наличия статистической информации получает закрепление в российском законодательстве» [6. С. 35].

Ресурсная концепция связывает уязвимость с состоянием бедности вследствие недостаточного доступа к материальным и нематериальным активам. Таким образом, учитывается наличие дополнительных активов, используя которые, можно выйти из кризисной ситуации. Однако при таком подходе понятие «актив» становится предельно широким, возникает вопрос о критериях «достаточности».

Социологическая концепция социального исключения или социальной эксклюзии (social exclusion) сосредотачивает внимание на разрыве социальных связей. По мнению социолога Э. Гидденса, исключение связано не с градациями неравенства, а с механизмами, которые действуют для отделения групп людей от основного социального потока [9].

Представление о природе социальной уязвимости, связанной с ограничением доступа к реализации уязвимыми группами населения своих прав, в концепции социального исключения близко к юридическому пониманию уязвимости.

В международном праве уязвимость индивида или группы населения означает более высокий, по сравнению с другими, риск стать жертвой нарушения прав человека, в том числе быть ограниченным в возможности реализовывать гарантированные каждому права и свободы [2. С. 500–511].

Признание международным сообществом тех или иных групп уязвимыми получило документальное оформление в соответствующих конвенциях, декларациях, иных документах. В институциональном плане ряд договорных органов ООН по правам человека сформирован специально для защиты прав уязвимых групп (женщин, инвалидов, трудящихся-мигрантов и др.)

По мнению Е. С. Алисиевич, на степень уязвимости индивида влияют внешние и внутренние факторы. К первым относятся войны и стихийные бедствия, глобализация, изменения климата. Внутренние факторы обусловлены субъективными характеристиками индивида, в том числе его возрастом, гендерной принадлежностью, расой, вероисповеданием, инвалидностью, которые по каким-то причинам вызывают у общества отторжение [2. С. 500– 511].

В. Г. Микрина основаниями отнесения лиц к уязвимым группам считает нарушение прав человека, отсутствие равноправия, дискриминацию, а к уязвимым группам работников в международном трудовом праве относит женщин, детей и подростков, трудящихся-мигрантов, инвалидов и домашних работников [3. С. 12–13, 16].

В российском трудовом праве понятие «уязвимые группы» не легализовано. Однако одним из оснований дифференциации правового регулирования фактически является уязвимость, которая связывается, как правило, с возрастом (работники в возрасте до 18 лет, работники предпенсионного возраста, работающие пенсионеры по старости (по возрасту)); полом (женщины), состоянием здоровья (инвалидность, беременность), семейными обязанностями. Возраст как фактор уязвимости работников в отечественном трудовом праве стал предметом самостоятельного исследования [1].

Учитывая, что автоматизация сильнее всего сказывается на представителях низкооплачиваемых профессий и усугубляет расовое и гендерное неравенство [4. С. 44–45], в отношении уязвимых групп работников можно отметить следующие риски внедрения ИИ:

– усиление дискриминации за счет внедрения дискриминирующих правил в алгоритмы ИИ системы и использовании их при приеме на работу, для оценки эффективности работников, расчета заработной платы, при направлении на обучение, принятии решений о применении дисциплинарных взысканий, включая увольнение; при этом вероятность массового нарушения прав уязвимых групп работников ввиду непрозрачности алгоритмов ИИ многократно усиливается;

– замена защищенных высокооплачиваемых рабочих мест временной низкооплачиваемой работой, которая не дает трудоправовых гарантий и через некоторое время тоже будет автоматизирована.

По мнению И. А. Филиповой, следствием изменений на рынке труда станет трансформация занятости населения, что вкупе с изменениями в отраслевой экономике и менеджменте, происходящими из-за увеличения доли виртуальной экономики, будет способствовать смене социального ландшафта [5].

В целом соглашаясь с указанными предложениями, следует отметить, что квотирование рабочих мест, если оно существенно сдерживает модернизацию производства, будет неэффективным. Вступая в соревнование с ИИ, люди, скорее

всего, неизбежно потерпят поражение. Поэтому переобучение работников необходимо, но не для того, чтобы конкурировать с ИИ, а для того, чтобы осваивать новые профессии.

Для снижения рисков дискриминации целесообразно:

– информировать работников о применении технологий ИИ, используемых работодателем;

– рассмотреть вопрос о предварительной (до начала использования) и последующей периодической верификации алгоритмов ИИ на предмет дискриминационных решений (в том числе посредством профсоюзного контроля);

– установить перечень кадровых решений, которые не могут быть приняты исключительно алгоритмами ИИ, а также перечень групп работников (прежде всего, уязвимых), в отношении которых решения таких алгоритмов подлежат обязательной проверке со стороны руководства;

– вернуться к идее о возложении на работодателя бремени доказывания в делах о дискриминации работника (или претендента на должность), если решение было принято ИИ.

Заключение. Автоматизация и ИИ – это объективные процессы, которые протекают все более стремительно, и их вряд ли возможно остановить. Один из способов предотвратить негативное развитие событий – начать процесс формирования справедливых рамок правового регулирования труда в новых условиях уже сейчас, повышая информированность работников относительно используемых в трудовом процессе алгоритмов ИИ, проверяя их на предмет дискриминационных решений, ограничивая желание работодателя при принятии кадровых решений целиком и полностью полагаться на ИИ.

Список литературы

1. Васильева Ю. В., Шуралева С. В. Возраст как фактор уязвимости работника в трудовом праве // Вестник Пермского университета. Юридические науки. 2020. № 49. С. 550-575.

2. Международное право: учебник для аспирантов. М.: РУДН, 2018. 648 с.

3. Микрина В. Г. Международно-правовые механизмы защиты трудовых прав наиболее уязвимых групп населения: дис. … канд. юрид. наук. М., 2018. 197 с.

4. Руз К. Устойчивы к будущему. 9 правил для людей в эпоху машин. М.: Ман, Иванов, Фербер, 2021. 256 с.

5. Филипова И. А. Создание метавселенной: последствия для экономики, социума и права // Journal of Digital Technologies and Law. 2023. Т. 1, № 1. С. 7-32. EDN LCCOJJ.

6. Шабунова А. А., Калачикова О. Н., Леонидова Г. В., Смолева Е. О. Эксклюзия как критерий выделения социально уязвимых групп населения // Экономические и социальные перемены: факту, тенденции, прогноз. 2016. № 2(44). С. 29-47.

7. Giddens A. The Third Way: The Renewal of Social Democracy. URL: https://yandex.ru

СОДЕРЖАНИЕ | CONTENTS

DIGITAL TECHNOLOGIES AND LAW

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ МЕЖДУНАРОДНО-ПРАВОВЫХ ОТНОШЕНИЙ | DIGITAL TECHNOLOGIES IN THE SYSTEM OF INTERNATIONAL-LEGAL RELATIONS

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ЧАСТНО-ПРАВОВЫХ (ЦИВИЛИСТИЧЕСКИХ) ОТНОШЕНИЙ | DIGITAL TECHNOLOGIES IN THE SYSTEM OF PRIVATE-LEGAL (CIVILISTIC) RELATIONS

ЦИФРОВЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ТРУДОВЫХ И СВЯЗАННЫХ С НИМИ ПРАВООТНОШЕНИЙ | DIGITAL TECHNOLOGIES IN THE SYSTEM OF LABOR AND ADJACENT RELATIONS

Научное издание

ЦИФРОВЫЕ ТЕХНОЛОГИИ И ПРАВО

Сборник научных трудов
II Международной научно-практической конференции

22 сентября 2023 г.
г. Казань

В шести томах
Том 5

Под редакцией И. Р. Бегишева, Е. А. Громовой, М. В. Залоило, И. А. Филиповой, А. А. Шутовой

Главный редактор *Г. Я. Дарчинова*
Редакторы: *Г. А. Тарасова, Е. А. Маннапова*
Технические редакторы: *О. А. Аймурзаева, С. Р. Каримова*
Дизайн обложки: *Г. И. Загретдинова*

ISBN 978-5-8399-0818-5

Подписано в печать 21.11.2023. Формат 60×84/16.
Гарнитура PT Astra Serif, 9. Усл. печ. л. 22,1. Уч.-изд. л. 28,1.
Тираж 500 экз. (1-й завод – 50 экз.) Заказ № 100.

Издательство «Познание» Казанского инновационного университета им. В. Г. Тимирясова
420111, г. Казань, ул. Московская, 42; тел. (843) 231-92-90; e-mail: zaharova@ieml.ru

Отпечатано с готового оригинал-макета в типографии ООО «ТЦО «Таглимат»
420108, г. Казань, ул. Зайцева, 17