ГОСУДАРСТВО И ПРАВО, 2022, № 11, с. 139–147
STATE AND LAW, 2022, No. 11, pp. 139–147

ИНФОРМАЦИОННОЕ ПРАВО И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

TRUST IN THE LAW DURING THE DIGITAL TRANSFORMATION

© 2022 T. A. Polyakova[1, *], V. B. Naumov[1, 2, **], A. V. Minbaleev[1, 2, *]**

[1]Institute of the State and Law of the Russian Academy of Sciences, Moscow
[2]Kutafin Moscow State Law University (MSAL)

**E-mail: polyakova_ta@mail.ru*
***E-mail: nau@russianlaw.net*
****E-mail: alexmin@bk.ru*

Received 13.10.2022

Abstract. This article raises the problem of society's and individuals' trust in the law during the digital transformation. It identifies factors that in many ways lead to decreased trust in the law. These factors include geopolitical crises and the changes the world experienced during the pandemic, as well as processes of poorer quality rulemaking, public administration, legal drafting and enforcement. It also identifies reasons why the law lags behind the realities of widespread use of new digital technologies in the XXI century, in which the number of gaps in the legal regulation system becomes critical for jurisprudence, legal theory, society and the state.

It has been found that increasing information pressure on the individual and the individual's openness and defenselessness to information flows, as well as stress and the infodemic, particularly during a pandemic and geopolitical crisis, destroy the ability to shape critical thinking. Due to overload, they deprive people of skills for effectively learning something new and developing creatively. Also, the more time the individual spends in the information space, subjected to powerful targeting technologies, the less right he or she has to choose. This is particularly the case now as the world is dominated by a couple dozen global digital platforms that provide people and small and medium business with an ever-expanding range of services, which means they no longer have the economic ability to choose other, alternative solutions.

The changes that have occurred in the system of people being forced to work remotely, "regulatory administration", the use of people's fear and confusion, have questioned the authority of the law. The article concludes that identifying information law's place in Russia and the modern world, including issues of the need to systematize information legislation for the country and society at a time when digital data are becoming the basis for a growing number of social interactions, seems to be one of the important processes to boost trust in the law as a social regulator.

The article raises issues of the legal regulation of the circulation of big data, the Internet of things, artificial intelligence and other digital technologies.

It analyzes a number of legal issues, including the generation of consistent hierarchical legal terminology for the Internet of things and a common vision of the system of IoT legal issues requiring new or modified solutions in light of industry specifics and the current state of the regulatory framework.

At the current stage of humanity's development, the "right to reject the use of digital technologies" could be a rational tool to strike a balance between individuals' rights and the public interest. Therefore, it will be important for achieving the goals of information law to create a system that protects the rights of those who are unable, unwilling or afraid to use new sophisticated technological solutions such as various cutting-edge digital technologies, including artificial intelligence technologies.

***Key words*:** trust in the law, big data, artificial intelligence, robotics, legal regulation, digital technologies, digital transformation, digital economy, development models.

For citation: *Polyakova, T.A., Naumov, V.B., Minbaleev, A.V. (2022).* Trust in the law during the digital transformation // Gosudarstvo i pravo=State and Law, No. 11, pp. 139–147.

This article was written as part of the state task on the topic "Legal regulation of the digital economy, artificial intelligence and information security".

DOI: 10.31857/S102694520022767-4

О ДОВЕРИИ К ПРАВУ В УСЛОВИЯХ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

© 2022 г. Т. А. Полякова[1, *], В. Б. Наумов[1, 2, **], А. В. Минбалеев[1, 2, *]**

[1]Институт государства и права Российской академии наук, г. Москва
[2]Университет им. О.Е. Кутафина (МГЮА)

**E-mail: polyakova_ta@mail.ru*
***E-mail: nau@russianlaw.net*
****E-mail: alexmin@bk.ru*

Поступила в редакцию 13.10.2022 г.

Аннотация. В статье поднимается проблема доверия общества и отдельных субъектов к праву в условиях цифровой трансформации. Выявлены факторы, приводящие во многом к снижению доверия к праву, в том числе как геополитические кризисы и изменения, проходившие в мире в условиях пандемии, так и процессы ухудшения качества нормотворчества, государственного управления и юридической техники и правоприменения. Выявлены причины отставания права от реалий массового использования новых цифровых технологий в XXI в., когда количество пробелов в системе правового регулирования приобретает для юридической науки, теории права, общества и государства критический характер.

Установлено, что увеличение информационного давления на личность, его открытость и беззащитность перед информационными потоками, стресс и инфодемия, особенно в условиях пандемии и геополитического перелома, разрушают возможность формирования критического мышления и за счет перегрузки лишают навыков эффективно узнавать новое и творчески развиваться, а все увеличивающееся по времени нахождение индивидуума в информационном пространстве в условиях мощных технологий таргетирования лишают его права выбора, особенно, когда сейчас в мире доминирует всего пара десятков глобальных цифровых платформ, оказывающих гражданам и мелкому и среднему бизнесу все более широкий спектр услуг, лишая их экономической возможности выбирать иные альтернативные решения.

Произошедшие изменения в системе принудительной работы в дистанционном формате, «подзаконное управление», использование страха и растерянности населения поставили вопрос об авторитете права. Делается вывод, что определение места информационного права в России и современном мире, включая проблематику необходимости систематизации информационного законодательства для страны и общества, когда цифровые данные становятся основой для возрастающего объема общественных отношений, представляется одним из важных процессов по обеспечению повышения доверия к праву как социальному регулятору.

Поднимаются проблемы правового регулирования оборота больших данных, интернета вещей, искусственного интеллекта и других цифровых технологий.

Анализируется целый ряд правовых вопросов, включая формирование непротиворечивой иерархической юридической терминологии в области интернета вещей и единого видения системы правовых проблем интернета вещей, требующих новых или измененных решений, с учетом отраслевой специфики и текущего состояния нормативной базы.

На современном этапе развития человечества разумным инструментом для достижения баланса прав граждан и публичных интересов может стать «право на отказ от использования цифровых технологий». В этой связи важной для реализации задачей информационного права является создание системы защиты прав лиц, не имеющих возможности или не желающих, или опасающихся использования новых сложных технологических решений, как, например, различные прорывные цифровые технологии, включая технологии искусственного интеллекта.

Ключевые слова: доверие к праву, большие данные, искусственный интеллект, робототехника, правовое регулирование, цифровые технологии, цифровая трансформация, цифровая экономика, модели развития.

Цитирование: *Polyakova, T.A., Naumov, V.B., Minbaleev, A.V. (2022).* Trust in the law during the digital transformation // Государство и право. 2022. № 11. С. 139–147.

Статья написана в рамках Государственного задания по теме «Правовое регулирование цифровой экономики, искусственного интеллекта информационной безопасности».

Over the past decade the law has come up against an entire system of challenges that have impacted its effectiveness and led to a decrease in trust in the law.

Factors shaping these processes could include geopolitical crises and the changes the world experienced during the pandemic, as well as processes of poorer quality rulemaking, public administration, legal drafting and enforcement. In this article, we will not dwell on subjective or sociopolitical causes. Rather, we will focus on circumstances that are an objective consequence of the law lagging behind the realities of widespread use of new digital technologies in the XXI century, in which the number of gaps in the legal regulation system becomes critical for jurisprudence, legal theory, society and the state.

For centuries, trust in the law has been based on the quality and consistency of how the law was applied as legal relationships changed slowly. The conservatism of this social regulator guaranteed trust in it and sources of entrenched social authority.

Everything began to change literally over a few decades of scientific and technological progress, of information and digital transformation. During that period the nature of social interactions has been undergoing cardinal changes for which the regulator was not prepared.

The content of the law relied on the "constants" of time, space, human will and its independence in the world as being seemingly immutable. However, this space became an information space already in the Internet age of the 1990[s] and was no longer split up by geography: the time and speed of electronic communications became "instant" in contrast to the "slow" interactions of past centuries. The digital world saw the rise of the phenomenon of autonomous systems with artificial intelligence technologies. In their digital interaction, humans can no longer be certain that they are interacting with subjects just like them, not with technologically generated "deep fake" images and sound. Digital systems are becoming so complex in their organization, so powerful at processing big data that the average person can no longer understand how they are used and they take on new features and functions of total control and identification even of those who want to preserve their "privacy." The realm of public administration, which always strives to control everything, and the "pyramid" of public administration that existed for millennia, are becoming either unnecessary or much less effective in a number of fields thanks to the appearance of "horizontal" peer-to-peer distributed registers. One confirmation of this is the increasingly popular area of decentralized financial technologies.

Increasing information pressure on the individual and the individual's openness and defenselessness to information flows, as well as stress and the infodemic, particularly during a pandemic and geopolitical crisis, destroy the ability to shape critical thinking. Due to overload, they deprive people of skills for effectively learning something new and developing creatively. Also, the more time the individual spends in the information space, subjected to powerful targeting technologies, the less right he or she has to choose. This is particularly the case now as the world is dominated by a couple dozen global digital platforms that provide people and small and medium business with an ever-expanding range of services, which means they no longer have the economic ability to choose other, alternative solutions.

The nature of the changes in digital interactions in the world in 2020–2021 is illustrative. During the COVID-19 pandemic the digital transformation was one of the world's officially proposed answers to the challenges of the time. This led to diverse processes where, on the one hand, there were more remote communication capabilities with a slightly greater degree of biomedical safety for people (an improvement that has yet to be fully evaluated). But, on the other hand, the quality of the related rulemaking and law enforcement went down and the system of civil-law rights and guarantees that had taken decades to create suffered[1].

Ultimately, the changes that have occurred in the system of people being forced to work remotely, "regulatory administration", the use of people's fear and confusion, have questioned the authority of the law. In this context, one of the important processes to boost trust in the law as a social regulator is to identify information law's place in Russia and the modern world, including issues of the need to systematize information legislation for the country and society at a time when digital data are becoming the basis for a growing number of social interactions.

It is conceivable that the modern world in its current form exists precisely thanks to data and, possibly, already in some ways for data rather than for humans. And, for information law, its key subject is information, including the variety of information that is data. Information itself is not an object of civil-law rights either in Russia (after that object was left out of Article 128 of the Russian Federation Civil Code in 2006) or almost anywhere else in the world. However, data are allowed to circulate.

Considering the nature of digital technologies that are being developed, data can be classified based on the definition of the particular processes of capturing and maintaining them. They can be presented simply as a Venn diagram where the following four key elements ("subsets") intersect: industrial data, big data, public data and personal data. Of greatest interest are issues of determining what is a general intersection and what is a specific intersection for the "subsets" of big and personal data. Four basic approaches to this can be identified in the world:

1. The EU has unified the protection of personal data and kept track of digital trends (in terms of big data processing).

2. The US has taken a sector-specific approach and has parallel regulation at the federal and state levels.

3. China has centralized control over big data and user data.

4. A hybrid system is developing in Russia combining approaches 1 and 3; however, some digital trends are ignored and there is no regulation of big data.

Each of these approaches broadly defines "personal data" so that personal data can be both data specifically relating to an individual and indirectly identifying that individual, for example, user activity data, IP addresses, online identifiers, and the like. In addition, each country has special requirements for information security. Fines for violating personal data laws differ in these systems but they vary within a system of two models: a fixed amount fine or a turnover fine on annual turnover or illegally earned income.

The following limitations are common regulatory barriers to the development of big data for each of these systems: 1) technical data are processed as personal data; 2) data processing is limited to pre-defined purposes within a database; 3) subjects have limited awareness of how the data are used and there is a need to align processing purposes with the text of user agreements; 4) decision-making is limited only on the basis of automated processing; 5) all organizational technical steps must be followed to protect data; 6) the sufficient degree of data anonymization

[1] See: *Kotov A., Naumov V.* E-Governance and Privacy in Pandemic Times // *Yang XS., Sherratt S., Dey N., Joshi A. (eds)* Proceedings of Sixth International Congress on Information and Communication Technology. Lecture Notes in Networks and Systems. Vol. 236. 2021. Springer, Singapore. P. 971–981. URL: https://doi.org/10.1007/978-981-16-2380-6_86

needs to be determined; 7) consents have to be gathered from data subjects.

Victor Naumov aptly states that "the regulatory status of big data generated by the huge number of information systems and devices could become one of the cornerstones of business and public administration. Moreover, its connection with different forms of privacy and nondisclosure requirements in the most varied types of legal relationships has yet to be defined. It is precisely big data that could 'turn the world upside down' in the future when identification will be done in the digital world using big data processing methods without direct participation in special legal relationships to identify subjects and, what is extremely dangerous, without informing those subjects"[2].

The combination of big data and artificial intelligence has become the subject and the first step for "game changing" regulation in the country, where laws on conducting experiments were passed two years ago. Those laws are Federal Law No. 122-FZ of 24 April 2020 "On Conducting the Experiment of Using Job-Related Electronic Documents" and Federal Law No. 123-FZ of 24 April 2020 "On Conducting the Experiment of Determining Special Regulation to Create the Necessary Conditions for the Development and Implementation of Artificial Intelligence Technologies in the Russian Federation Constituent Entity of the Federal City of Moscow and Amending Articles 6 and 10 of the Federal Law "On Personal Data"". Key in these new laws, including for data and the general task of identifying objects and subjects, was the authorization of the processing of individual's personal data without obtaining their prior consent.

The same initiative is being developed for the Internet of things, whose regulation deserves separate attention. One of the most realistic definitions of the term "Internet of things" was presented in item 3.2.2 of the International Telecommunication Union's Recommendation ITU-T Y.2060 (06/2012), pursuant to which the Internet of things is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies"[3]. The authors of the ITU Recommendation aptly note that "through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled... from a broader perspective, the IoT can be perceived as a vision with technological and societal implications"[4].

There are currently a number of legal issues, including the generation of consistent hierarchical legal terminology for the Internet of things and a common vision of the system of IoT legal issues requiring new or modified solutions in light of industry specifics and the current state of the regulatory framework. Several years ago, researchers, including author V.B. Naumov, developed the "Open Concept of Regulation of the Internet of Things"[5] that proposes creating an open register of IoT devices and solutions based on that technology "organized according to the principle of voluntary declaration. The register could contain information about the capabilities of various devices in terms of information gathering and automated connectivity with other devices. Such a register could include elements of self-regulation..."[6].

It should be acknowledged that the Internet of things is a tool for sharply decreasing privacy where a humanity "covered with sensors" carries huge masses of not just data but big data as part of its daily life, "measuring" all material space and making the task of digital identification in the real world entirely achievable.

These challenges are directly related to the issues of organizing the circulation of big data mentioned above. This is also noted by other authors, who point to the trend of personal data anonymization becoming less valuable in a situation where it is statistically possible to get other "secondary" data from an increasing number of other sources[7].

The legal regulation in this area could evolve in different ways. First, the concept of identification privacy could be developed[8]. Second, there could be an attempt to detail (as, for example, in Japan) the legal regulation for different types of data depending on how they are obtained and processed. This objectively requires that the importance of different types of technologies for the economy and the state be prioritized. Third, a combined approach is possible. It would involve activating statutory and technical regulation of the field, providing regulatory support for general provisions (e.g., concepts, general principles, requirements to subjects) on the circulation of big data, and using citations in laws and regulations to statutory and technical acts on a number of issues. Combined regulation also involves supplementing a number of laws and regulations supporting the circulation of big data, including the laws on personal data, communications, administrative offenses, certification and metrology, and making changes to the OKVED (Russian Classification of Economic Activities), etc. It is also important to develop state support measures and, similarly to artificial intelligence, to explore the issue of developing and adopting a special code of ethics.

Data, including personal data, are aggregated in the world on unimaginably large scales. In addition to states, transnational digital platforms such as Google Inc., various social networks,

---

[2] *Naumov V.B.* Organizational and legal analysis of the development of commercial digital identification systems // Leningrad Law Journal. 2020. No. 1 (59). P. 61.

[3] See: ITU-T Recommendation Y.2060 (06/2012). Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks. Next Generation Networks – Frameworks and functional architecture models. Overview of the Internet of things. URL: https://www.itu.int/rec/T-REC-Y.2060–201206-I (accessed: 26.09.2022); ITU-T Recommendation Y.2069. Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks. Next Generation Networks – Frameworks and functional architecture models. URL: https://www.itu.int/rec/T-REC-Y.2069-201207-I/en (accessed: 26.09.2022).

[4] Populyarnost Internet veshchei tol'ko rastet [The Popularity of the Internet of Things is Only Growing]. Internet of Things. Conference. Expo. Meetup. 29 August 2016 (World Trade Center, Moscow), based on Vedomosti.ru materials. URL: http://iotconf.ru/ru/news/populyarnost-interneta-veshchey-tolko-rastet#sthash.nGv1B8Sw.yfl7JvOb.dpbs (accessed: 26.09.2022).

[5] *Naumov V.B., Arkhipov V.V., Pchelintsev G.A. et al.* Open concept "Internet of Things: legal aspects (Russian Federation)". Version 2.0. For public discussion // Law and information: questions of theory and practice: collection of works International Scientific and Practical Conference. Electronic legislation. Collections of the Presidential Library / scientific ed. by N.A. Sheveleva. 2019. P. 162–194.

[6] *Arkhipov V.V., Naumov V.B., Pchelintsev G.A., Chirko Ya. A.* Open concept of regulation of the Internet of Things // Information Law. 2016. No. 2. P. 18–25.

[7] See: *Savelyev A.I.* Problems of application of legislation on personal data in the era of 'Big Data" (Big Data) // Law. Journal of the Higher School of Economics. 2015. No. 1. P. 54–61.

[8] For more detail see: *Naumov V.B.* The task of ensuring the secrecy of identification in information law // Monitoring of law enforcement. 2019. No. 3. P. 70–75.

Amazon, Alibaba and others are key data controllers. These processes can be illustrated by the following facts: 1) there are more social media users than the populations of China and India; 2) Internet companies' revenues frequently exceed the GDP of very many countries of the world; 3) states are actively trying to regulate their activities and contact them directly with requests; 4) those companies' data breaches affect a large number of people (the Yahoo data breach affected hundreds of millions of user accounts). And it should be noted that 20 of the world's largest companies capturing and processing data are located in only two countries: the United States and China. This is undoubtedly already affecting geopolitical processes in the world.

Therefore, data can be a subject of competition and big IT companies' activities must be regulated by antitrust laws, among others. Antitrust laws must take account of the features of the digital services market. Also, given the fact that those companies may not have subdivisions or representative offices in a country, some countries actively use the possibility of extraterritorial application of laws to companies whose activities are targeted at people from those countries. This approach was used in such countries as the United States, the European Union, Turkey and China, and Russia has joined them in recent years.

In general, both in supporting competition or information security and the circulation of digital data, as well as in the general area of state control and supervision of all subject-specific relations, the role of the state will grow, as will the creation of complicated (and, likely, non-transparent) partnerships with leading IT businesses in various regions of the world.

The issues of artificial intelligence technologies already mentioned have also become a commonly acknowledged subject of discussion and analysis and, gradually, rulemaking. And, as there is no broad legal enforcement, it can be considered that the legal relationships for using artificial intelligence technologies can't yet be called widespread and publicly significant, in contrast to the circulation of data.

A study conducted by Dentons law firm globally in 2021 among more than 215 business communities[9] yielded the following results. More than 60% of companies use or test artificial intelligence (AI) systems in their operations. Of those, only 12% actively use AI in their operations, while the other 48% are at the initial stage of implementing pilot programs in various areas of their activity. The most popular areas are CRM systems (24%), administration of business processes (19%) and sales (18%).

As for problems associated with applying artificial intelligence, respondents noted the following collection of answers that creates risks for them:

1) cost of AI systems – 83%;

2) data protection – 81%;

3) the human role of controlling the AI system decision-making process – 81%;

4) uncertainty of the rules used to determine who is responsible for AI actions or errors – 80%;

5) inability to explain AI decisions – 76%;

6) weak data architecture or low quality of data – 76%;

7) lack of clear statutory regulation – 75%;

8) uncertainty as to the applicable legal regime – 74%;

9) dependence on AI supplier – 74%;

10) insufficient understanding of AI capabilities – 68%;

11) lack of trust in AI – 68%;

12) lack of mandatory liability insurance – 59%;

13) possible discrimination when delegating decision-making to AI – 57%.

The study also found that the representatives of the companies that responded to the survey also expect regulators to provide security mechanisms for using AI. Priorities are confidentiality (61%), consumer protection (52%), and criminal liability (46%). At the same time, business shows poor knowledge of the laws. Depending on the field of law, between 55% and 75% of respondents don't know the relevant laws or even whether such laws exist in their jurisdiction; 63% of respondents don't know which government body is authorized to regulate AI in their country.

In Russia the first tailored piece of legislation regulating artificial intelligence was passed in 2019[10]. The regulatory framework hasn't changed much since then, other than a few acts permitting the testing of artificial intelligence technology in limited conditions. So far, this is due to the low importance of subject-specific relationships and poor elaboration of the related issues, which gives rise to many empty and / or fruitless discussions. Unfortunately, there are also extremely few specific proposals regarding general regulation of interactions in the field of artificial intelligence, and regulation of certain aspects of the use of those technologies, including in the public and social sectors. However, work is underway in the European Union, the United States and a number of other states to approve final versions of acts that will regulate artificial intelligence.

Terminology issues are particularly well illustrated in the field of robotics, where there are currently different types of confusion. The conceptual framework in the area needs to be organized with due consideration for the features of artificial intelligence technologies, the categories of cyberphysical and information systems and robots, and the degree and nature of their involvement in social interactions[11]. It is important to determine whether the definitions in statutory and technical acts can be used, including when developing the conceptual framework for certain areas where artificial intelligence will be applied.

A cyberphysical system is primarily an information system that is integrated into a physical component and which has information elements. A robot is a mechanism that has a physical basis, is artificial (from the biological perspective it does not possess

[9] See: Iskusstvenny intellekt primenyayut 60% krupnykh i srednikh kompanii [Sixty Percent of Large and Medium Companies Use Artificial Intelligence], Vedomosti, 12 January 2022. URL: https://www.vedomosti.ru/technology/articles/2022/01/12/904347-iskusstvennii-intellekt-primenyayut-60-kompanii (accessed: 03.09.2022).

[10] See: Russian Federation Presidential Decree No. 490 of 10 October 2019 "On the Development of Artificial Intelligence in the Russian Federation" (together with the "National Strategy for Developing Artificial Intelligence 2030").

[11] See: *Arkhipov V.V., Gracheva A.V., Naumov V.B. et al.* Definition of artificial intelligence in the context of the Russian legal system: a critical approach // State and Law. 2022. No 1. P. 168–178; *Polyakova T.A., Minbaleev A.V., Krotkova N.V.* The main trends and problems of the development of the science of Information Law // State and Law. 2022. No. 9. P. 94–104. DOI: 10.31857/S102694520022203-4; *Polyakova T.A., Troyan N.A.* Formation of scientific and legal approaches to the development of the system of application of digital technologies in rulemaking // Legal policy and legal life. 2022. No. 1. P. 43–58; Legal and ethical aspects related to the development and application of artificial intelligence and robotics systems: history, current state and prospects of development / V.V. Arkhipov, G.G. Kamalova, V.B. Naumov et al. St. Petersburg, 2020.

animate features) and has a minimal degree of autonomy of action. Artificial intelligence is primarily a program / algorithm that is capable of analyzing information about the environment, possesses a certain degree of autonomy, is capable of self-learning and has such a quality as intellectuality, which enables it to imitate human activity. So, for many decades the approaches to classifying artificial intelligence routinely distinguished between "strong AI" and "weak AI". The former can acquire the ability to think and be self-aware at least at a human level, and is capable of self-learning. The latter is used in a highly specialized way and can only surpass humans in a specific area.

Currently, the discussion of the legal status of robots and AI is developing most vividly and "with imagination" in two areas: 1) to declare that a robot and / or artificial intelligence are an object of law (a special type of thing, an agent acting for itself or on behalf of an owner, or a legal entity's property created by the robot's owner); 2) to declare a robot or AI a subject and, possibly, a quasi-subject (there are close analogies for this: the robot as an animal, legal entity or electronic agent, the robot as a human). These discussions have already resulted in the development of several draft documents in Russia.

According to an old (2016) draft of amendments to the Russian Civil Code, "*a robot-agent is a robot that is intended to engage in civil transactions by decision of the owner and due to its design features. A robot-agent has its own property and is liable with that property for its obligations, can acquire and exercise civil-law rights and bear civil-law obligations* sui juris"[12].

In another well-known document, the "Model Convention on Robotics and Artificial Intelligence"[13], developed in Russia in 2017, the authors decided not to propose a special legal definition and combined the existing regulatory approaches in it: a black box and a red button for robots, the problems of safety and confidentiality. New suggestions were made in legal and ethical regulation: to identify a category of high-risk robots, to establish the presumption that artificial intelligence is dangerous, and to require conscious interaction with it. The first suggestions to regulate military robots and for international cooperation were made. To show how the topic has been elaborated, we will indicate some of the theses from that document. Each of them could become the subject of broad academic discussion.

Four approaches to liability for robots' actions being discussed at this stage of development can currently be identified:

release from liability for the actions of the robot (or information system with artificial intelligence) but with appropriate compensation being paid, including using insurance against risks;

no-fault liability of its manufacturer;

liability depending on the fault of the subject, i.e., the manufacturer or owner;

the robot bears liability (its owner is liable similarly to how the founder of a legal entity bears liability).

In all of these approaches the future legal definition of artificial intelligence (defined in a statute) is of critical importance. In light of the latest achievements in legal research on the subject the author proposes using the following definition for these purposes:

"*Artificial Intelligence is an information system the results of whose functioning are unpredictable for humans because the system is capable of determining on its own how its assigned tasks should be solved (including by using self-learning technologies)*"[14].

Now, when organizing the circulation of any new widespread digital technologies the difficult issue of trust in those technologies needs to be considered. If this is not done, a robust digital environment of trust cannot be created where participants will act consciously and will have a set of rights and guarantees.

For example, when using digital technologies, including artificial intelligence, it is important to know that they are being used, who their developers are, and the main features of using them. Legal rules also need to be established that would stipulate the liability of developers and operators of artificial intelligence technologies. In addition, the requirement of "self-identification of devices and solutions based on artificial intelligence technologies when interacting with a human and citizen on issues affecting their rights, freedoms and legitimate interests" should be met[15].

The same requirements for ensuring the necessary degree of trust in communications arise when using virtual and augmented reality technologies. There, the determination of which objects and subjects are participating and the extent to which they can be identified directly affect the ability to protect people's rights in the virtual space and hold people liable under the law.

Let's also not forget that civil-law regulation continues to play an important role in a virtual reality, where additive technologies are becoming more popular[16], and in general in almost any area where new digital technologies are created and used. In particular, issues of ensuring that intellectual property can circulate. The legal regulation in this area is becoming even more complicated compared to the commonly used Internet and what have already become widespread technologies of exchanging digital information. Here we can identify new problems of determining the status of the "creativity" of artificial intelligence[17], the circulation of models for 3D printing, integrated rights to avatars in virtual worlds, and much else.

The problems and related tasks of future legal regulation in cutting-edge digital technologies of the digital transformation, here considered on the example of big data and artificial intelligence, will naturally dovetail with current applied areas of legal assistance in building digital platforms.

Digital platforms are created using a large number of resources and a variety of different information (digital) technologies. Most importantly, they involve many partner organizations, usually leaders in one or another area of technological development and / or implementation.

---

[12] *Arkhipov V.V., Naumov V.B.* Artificial intelligence and autonomous devices in the context of law: on the development of the first law on robotics in Russia // Proceedings of SPIIRAN. 2017. No. 6 (55). P. 54. See the draft of the Federal Law "On Amending the Russian Federation Civil Code to Improve the Legal Regulation of Robotics Relations".

[13] See: *Naumov V.B., Neznamov A.V.* Model convention on robotics and artificial intelligence. Rules for the creation and use of robots and artificial intelligence // Law and information: questions of theory and practice: collection works VII International Scientific and Practical Conference. Electronic Legislation / scientific ed. N.A. Sheveleva. 2017. P. 210–220.

[14] *Arkhipov V.V., Braginets A. Yu., Gracheva A.V., Naumov V.B.* On the way to the legal definition of artificial intelligence // Information Law. 2021. No. 4. P. 24.

[15] See: *Naumov V.B.* Institute of identification in Information Law: abstract ... Doctor of Law. M., 2020. P. 18.

[16] For more detail on the legal issues see *Akhobekova R.A., Zagorodnaya A.A., Naumov V.B.* Problems of legal regulation of three-dimensional printing // Law. 2017. No. 4. P. 90–102.

[17] See: *Naumov V.B., Tytyuk E.V.* On the issue of the legal status of "creativity" of artificial intelligence // Jurisprudence. 2018. Vol. 62. No. 3. P. 531–540.

The complex combination of objects and subjects in this field gives rise to an entire "ecosystem" for a particular digital platform. The first issues to be subjected to legal analysis in this field should be the choice of models for interaction between partners, the creators and operators of a platform; information and cybersecurity; intellectual property rights management; government relations (e.g., licensing and certification, control and supervision in the broad sense), and legitimate questions of commercialization and scaling up a digital platform and technologies used.

There are three models for interaction between key partners: 1) the "centralized model" (where all partners delegate decision-making authority to a single platform operator); 2) the "two keys model," where some key partners make decisions together with the platform operator(s); 3) the "distributed model," where each partner has the right to make its own decisions. A balance should be sought when choosing an appropriate model: legal, technological, commercial and other risks need to be considered. In practice, contracts, partnerships, joint ventures and the "open source" model (for regulating issues of intellectual property use) can be used to build the model.

When it comes to digital platforms, their creation and how partners use them to carry out their activity, many different legal issues arise. They can be classified by their legal substance and the types of technologies.

In Information Law, some of these are:

information access issues in general, and to big data, in particular;

the liability of information brokers and other key partners involved in the digital platform's ecosystem;

the legal treatment of user data and big data on the platform and their localization;

personal data processing;

the legal status of the "organizer of dissemination of information";

regulatory issues of the laws on communications and the related subject of certification and licensing;

protection and confidentiality of information;

regulatory issues of advertising laws.

In the related area of intellectual property, key issues will be:

the holding of exclusive rights to a platform's components;

issues of having clean licenses to the platform's objects;

the legal status of digital models and other new forms of intellectual property;

open-source use policy when developing, using and replicating technology solutions in related areas of application;

the problem of derivative works and the criteria for "new" objects;

licensing of rights in the digital platform ecosystem.

Legal issues related to the following may come up when interacting with developer partners:

resolution of conflicts and identification of grounds for terminating contracts between them;

guarantees of information integrity and continuous operation of the digital platform, the types of services provided by the platform and responsibility for the quality of those services;

commercial dependence on suppliers of IT solutions and / or third parties.

Other issues worthy of attention are how antitrust laws are enforced, fighting user discrimination and the imposition of related information services[18]. Given today's realities, risks related to sanctions laws will also have to be followed.

At the same time, it should be concluded that in the absence of a developed legal terminology and given the systemic lacunae in laws on digital transformation, it will be difficult to solve the legal problems and tasks facing government and business, including when providing legal support for the creation and operation of digital platforms.

It is also very important when choosing legal models to regulate digital technologies and remove the barriers that have been identified and fill the gaps in legislation to use interdisciplinary expertise and make decisions based on the strategic interests of the state and society considering the processes of deglobalization that the world is already undergoing. In this context, one essential task could be to establish a system of statutory requirements to arrange for mandatory integrated expert examination and assessment of the consequences of widespread introduction of one or another digital technology (including using comprehensive modeling of the future state of society).

In the digital transformation field, there is yet another important social and legal aspect requiring attention. At a minimum, humans and citizens need to be afforded the right to make a conscious choice whether or not to use digital technologies (information technologies that are, for the sake of discussion, more sophisticated than those currently existing: technologies without big data, artificial intelligence and virtual worlds). Here, at the current stage, it seems inadmissible to follow the practice of heedlessly introducing "ideals" of total e-document flow and the ever more widespread unconditional rejection of in-person and/or paper-based interaction between government authorities and individuals. It evolved when the use of classic information technologies was inconsistent and people had a low level of technological literacy.

At the current stage of humanity's development, the "right to reject the use of digital technologies" could be a rational tool to strike a balance between individuals' rights and the public interest. If people had this right, the state would be obligated to provide (or require that business entities using them commercially provide) an equivalent alternative to using technical devices in areas that most affect a subject's rights and freedoms[19].

Therefore, it will be important for achieving the goals of information law to create a system that protects the rights of those who are unable, unwilling or afraid to use new sophisticated technological solutions such as various cutting-edge digital technologies, including artificial intelligence technologies. Achieving this goal should not repeat the struggle with the phenomenon well-known for more than two decades of digital (information) inequality. It has still been impossible to achieve serious success in that struggle, and social groups are still segregated in a number of countries of the world by their access to information technologies.

How should the legislation evolve in these conditions?

---

[18] In this subject matter in Russia the Federal Antimonopoly Service's actions against Bayer and Monsanto can be highlighted, and there was a similar antitrust ruling in the European Union against the joint venture of Telefonica UK, Vodafone UK and Everything Everywhere.

[19] See: *Naumov V.B.* Rejection of digital technologies: absurdity or a new human and citizen right // The Fourth Bachilov Readings: materials of the International Scientific and Practical Conference / ed. T.A. Polyakov, A.V. Minbaleev, V.B. Naumov. M., 2022. P. 83.

In past decades we could have limited ourselves to amending existing laws, including by identifying barriers preventing the effective development and dissemination of technologies, and removing those barriers. Both in this model and for other scenarios of rulemaking development it should be accompanied by an overall assessment of the risks of the most defenseless and weak members: individuals. The modern rights of humans and citizens should be protected and new legal solutions should be proposed.

A second development model could be the appearance of new laws, stand-alone pieces of legislation with a unique subject matter and area of legal regulation. Although this methodology seems progressive, it is already outdated because the multifaceted issues of digital data circulation will require a convergence of "old" laws and the regulation of digital technologies. So, the authors are of the opinion that at the current stage of the digital transformation during an era of geopolitical and socioeconomic changes the ideas of codifying subject-specific legislation should be followed.

It appears that the questions posed by modern jurisprudence and practice in the legal regulation of creating and using cutting-edge digital technologies already "deserve" a separate systemic piece of legislation. The delayed start of public work on that legislation is becoming all the more noticeable in society.

All of the issues discussed in this article will help to achieve the critically important objective of creating the necessary degree of trust both when digital technologies are created and used, and to enhance the role of the law at the current stage of development of society and the state.

REFERENCES

1. *Arkhipov V.V., Braginets A. Yu., Gracheva A.V., Naumov V.B.* On the way to the legal definition of artificial intelligence // Information Law. 2021. No. 4. P. 24 (in Russ.).
2. *Arkhipov V.V., Gracheva A.V., Naumov V.B. et al.* Definition of artificial intelligence in the context of the Russian legal system: a critical approach // State and Law. 2022. No. 1. P. 168–178.
3. *Arkhipov V.V., Naumov V.B.* Artificial intelligence and autonomous devices in the context of law: on the development of the first law on robotics in Russia // Proceedings of SPIIRAN. 2017. No. 6 (55). P. 54 (in Russ.).
4. *Arkhipov V.V., Naumov V.B., Pchelintsev G.A., Chirko Ya.A.* Open concept of regulation of the Internet of Things // Information Law. 2016. No. 2. P. 18–25 (in Russ.).
5. *Akhobekova R.A., Zagorodnaya A.A., Naumov V.B.* Problems of legal regulation of three-dimensional printing // Law. 2017. No. 4. P. 90–102 (in Russ.).
6. *Kotov A., Naumov V.* E-Governance and Privacy in Pandemic Times // *Yang XS., Sherratt S., Dey N., Joshi A. (eds)* Proceedings of Sixth International Congress on Information and Communication Technology. Lecture Notes in Networks and Systems. Vol. 236. 2021. Springer, Singapore. P. 971–981. URL: https://doi.org/10.1007/978-981-16-2380-6_86
7. Legal and ethical aspects related to the development and application of artificial intelligence and robotics systems: history, current state and prospects of development / V.V. Arkhipov, G.G. Kamalova, V.B. Naumov et al. St. Petersburg, 2020 (in Russ.).
8. *Naumov V.B.* Institute of identification in Information Law: abstract ... Doctor of Law. M., 2020. P. 18 (in Russ.).
9. *Naumov V.B.* Organizational and legal analysis of the development of commercial digital identification systems // Leningrad Law Journal. 2020. No. 1 (59). P. 61 (in Russ.).
10. *Naumov V.B.* Rejection of digital technologies: absurdity or a new human and citizen right // The Fourth Bachilov Readings: materials of the International Scientific and Practical Conference / ed. T.A. Polyakov, A.V. Minbaleev, V.B. Naumov. M., 2022. P. 83 (in Russ.).
11. *Naumov V.B.* The task of ensuring the secrecy of identification in Information Law // Monitoring of law enforcement. 2019. No. 3. P. 70–75 (in Russ.).
12. *Naumov V.B., Arkhipov V.V., Pchelintsev G.A. et al.* Open concept "Internet of Things: legal aspects (Russian Federation)". Version 2.0. For public discussion // Law and information: questions of theory and practice: collection of works International Scientific and Practical Conference. Electronic legislation. Collections of the Presidential Library / scientific ed. by N.A. Sheveleva. 2019. P. 162–194 (in Russ.).
13. *Naumov V.B., Neznamov A.V.* Model convention on robotics and artificial intelligence. Rules for the creation and use of robots and artificial intelligence // Law and information: questions of theory and practice: collection works VII International Scientific and Practical Conference. Electronic Legislation / scientific ed. N.A. Sheveleva. 2017. P. 210–220 (in Russ.).
14. *Naumov V.B., Tytyuk E.V.* On the issue of the legal status of "creativity" of artificial intelligence // Jurisprudence. 2018. Vol. 62. No. 3. P. 531–540 (in Russ.).
15. *Polyakova T.A., Minbaleev A.V., Krotkova N.V.* The main trends and problems of the development of the science of Information Law // State and Law. 2022. No. 9. P. 94–104. DOI: 10.31857/S102694520022203-4 (in Russ.).
16. *Polyakova T.A., Troyan N.A.* Formation of scientific and legal approaches to the development of the system of application of digital technologies in rulemaking // Legal policy and legal life. 2022. No. 1. P. 43–58 (in Russ.).
17. *Savelyev A.I.* Problems of application of legislation on personal data in the era of 'Big Data" (Big Data) // Law. Journal of the Higher School of Economics. 2015. No. 1. P. 54–61 (in Russ.).

СПИСОК ЛИТЕРАТУРЫ

1. *Архипов В.В., Брагинец А.Ю., Грачева А.В., Наумов В.Б.* На пути к юридическому определению искусственного интеллекта // Информационное право. 2021. № 4. С. 24.
2. *Архипов В.В., Наумов В.Б.* Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике // Труды СПИИРАН. 2017. № 6 (55). С. 54.
3. *Архипов В.В., Наумов В.Б., Пчелинцев Г.А., Чирко Я.А.* Открытая концепция регулирования интернета вещей // Информационное право. 2016. № 2. С. 18–25.
4. *Ахобекова Р.А., Загородная А.А., Наумов В.Б.* Проблемы правового регулирования трехмерной печати // Закон. 2017. № 4. С. 90–102.
5. *Наумов В.Б.* Задача обеспечения тайны идентификации в информационном праве // Мониторинг правоприменения. 2019. № 3. С. 70–75.
6. *Наумов В.Б.* Институт идентификации в информационном праве: автореф. дис. ... д-ра юрид. наук. М., 2020. С. 18.
7. *Наумов В.Б.* Организационно-правовой анализ развития коммерческих цифровых систем идентификации // Ленинградский юрид. журнал. 2020. № 1(59). С. 61.
8. *Наумов В.Б.* Отказ от цифровых технологий: абсурд или новое право человека и гражданина // Четвертые Бачиловские чтения: материалы Междунар. науч.-практ. конф. / отв. ред. Т.А. Полякова, А.В. Минбалеев, В.Б. Наумов. М., 2022. С. 83.
9. *Наумов В.Б., Архипов В.В., Пчелинцев Г.А. и др.* Открытая концепция «Интернет вещей: правовые аспекты (Российская Федерация)». Версия 2.0. Для публичного обсуждения // Право и информация: вопросы теории и практики: сб. тр. Междунар. науч.-практ. конф. Сер. «Электронное законодательство». Сборники Президентской библиотеки / науч. ред. Н.А. Шевелёва. 2019. С. 162–194.

10. *Наумов В.Б., Незнамов А.В.* Модельная конвенция о робототехнике и искусственном интеллекте. Правила создания и использования роботов и искусственного интеллекта // Право и информация: вопросы теории и практики: сб. тр. VII Междунар. науч.-практ. конф. Сер. «Электронное законодательство» / науч. ред. Н.А. Шевелёва. 2017. С. 210–220.

11. *Наумов В.Б., Тытюк Е.В.* К вопросу о правовом статусе «творчества» искусственного интеллекта // Правоведение. 2018. Т. 62. № 3. С. 531–540.

12. *Полякова Т.А., Минбалеев А.В., Кроткова Н.В.* Основные тенденции и проблемы развития науки информационного права // Государство и право. 2022. № 9. С. 94–104. DOI: 10.31857/S102694520022203-4

13. *Полякова Т.А., Троян Н.А.* Формирование научно-правовых подходов к развитию системы применения цифровых технологий в нормотворчестве // Правовая политика и правовая жизнь. 2022. № 1. С. 43–58.

14. Правовые и этические аспекты, связанные с разработкой и применением систем искусственного интеллекта и робототехники: история, современное состояние и перспективы развития / В.В. Архипов, Г.Г. Камалова, В.Б. Наумов и др. СПб., 2020.

15. *Савельев А.И.* Проблемы применения законодательства о персональных данных в эпоху «Больших данных» (Big Data) // Право. Журнал ВШЭ. 2015. № 1. С. 54–61.

16. *Arkhipov V.V., Gracheva A.V., Naumov V.B. et al.* Definition of artificial intelligence in the context of the Russian legal system: a critical approach // State and Law. 2022. No. 1. P. 168–178.

17. *Kotov A., Naumov V.* E-Governance and Privacy in Pandemic Times // *Yang XS., Sherratt S., Dey N., Joshi A. (eds)* Proceedings of Sixth International Congress on Information and Communication Technology. Lecture Notes in Networks and Systems. Vol. 236. 2021. Springer, Singapore. P. 971–981. URL: https://doi.org/10.1007/978-981-16-2380-6_86

Authors' information

POLYAKOVA Tatyana A. –
Doctor of Law, Professor, chief researcher, Acting Head of the Information Law and International Information Security Sector, Institute of State and Law of the Russian Academy of Sciences;
10 Znamenka str., 119019 Moscow, Russia

NAUMOV Victor B. –
Doctor of Law, associate Professor, chief researcher of the Information Law and International Information Security Sector, Institute of State and Law of the Russian Academy of Sciences;
10 Znamenka str., 119019 Moscow, Russia; chief researcher of the Laboratory of Applied Informatics and Problems of Society Informatization of the St. Petersburg Federal Research Center of the Russian Academy of Sciences; 39, 14th line of V.I., 199178 St. Petersburg, Russia

MINBALEEV Alexey V. –
Doctor of Law, associate Professor, Head of the Department of Information Law and Digital Technologies of Kutafin Moscow State Law University (MSAL); 9 Sadovaya-Kudrinskaya str., 125993 Moscow, Russia; chief researcher, Information Law and International Information Security Sector, Institute of State and Law of the Russian Academy of Sciences; 10 Znamenka str., 119019 Moscow, Russia

Сведения об авторах

ПОЛЯКОВА Татьяна Анатольевна –
доктор юридических наук, профессор, главный научный сотрудник, и.о. заведующей сектором информационного права и международной информационной безопасности Института государства и права РАН; 119019 г. Москва, ул. Знаменка, д. 10
SPIN-код: 4224-3174, AuthorID: 732015
ORCID: 0000-0003-3791-2903

НАУМОВ Виктор Борисович –
доктор юридических наук, доцент, главный научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права Российской академии наук; 119019 г. Москва, ул. Знаменка, д. 10; главный научный сотрудник Лаборатории прикладной информатики и проблем информатизации общества Санкт-Петербургского федерального исследовательского центра РАН; 199178 г. Санкт-Петербург, 14-я линия В.О., д. 39
SPIN-код: 5729-5413, AuthorID: 6101
ORCID: 0000-0003-3453-6703

МИНБАЛЕЕВ Алексей Владимирович –
доктор юридических наук, доцент, заведующий кафедрой информационного права и цифровых технологий Московского государственного юридического университета им. О.Е. Кутафина (МГЮА); 125993 г. Москва, Садовая-Кудринская ул., д. 9; главный научный сотрудник сектора информационного права и международной информационной безопасности Института государства и права РАН; 119019 г. Москва, ул. Знаменка, д. 10
SPIN-код: 7148-1527, AuthorID: 651824
ORCID: 0000-0001-5995-1802