ORIGINAL PAPER

DOI: 10.26794/2587-5671-2022-26-3-169-185
UDC 349;336.1;369.06(045)
JEL K32, G22, I18

Organizational, Legal and Financial Aspects of Digitalization and Implementation of Artificial Intelligence Technologies in Healthcare

M.A. Lapina
Financial University, Moscow, Russia

ABSTRACT

The paper aims to substantiate the main development directions of legal regulation of artificial intelligence in healthcare. The main hypothesis of the study is the assumption that artificial intelligence should not be a subject of law. The author formulates the postulates necessary for the introduction of modern technologies in the context of the digitalization of medicine. General and special scientific methods are used: the dialectical method of cognition of reality, synthesis and deduction. The comparative and formal legal method of scientific cognition made it possible to analyze the laws and other documents of a number of states in the field of digitalization and the mechanism for financing the provision of medical services and medical care. The article analyzes the directions proposed by scientists and practitioners with the participation of the largest IT companies to improve the provision of medical care and medical services and optimize healthcare management. The author draws attention to financial mechanisms to stimulate the introduction of digital technologies in the healthcare system, directly to the provision of medical care. Structuring the main directions of applicability of digital technologies in healthcare allowed us to formulate proposals for improving their legal support. The analysis of foreign and domestic legislation has revealed the importance of using such a financial and legal mechanism as health insurance. Based on the results of the study, the author makes a conclusion about the need for a systematic approach to digitalization in healthcare and proposes an institutional and legal model for the development of patient-centered medicine based on artificial intelligence technologies.

Keywords: healthcare; artificial intelligence; health insurance; medical ethics; financing; digital technologies

For citation: **Lapina M.A. Organizational, legal and financial aspects of digitalization and implementation of artificial intelligence technologies in healthcare. *Finance: Theory and Practice.* 2022;26(3):169-185. DOI: 10.26794/2587-5671-2022-26-3-169-185**

INTRODUCTION

Russia has adopted a policy of developing the information society and increasing the effectiveness of State authorities in all spheres of life by integrating certain achievements in the development of digital technologies and artificial intelligence (hereinafter — AI).

Among domestic researchers the most systemically revealed the legal basis of artificial intelligence technologies P.M. Morkhat in the monograph "Artificial intelligence: a legal view" in 2017 [1]. One of the first attempts to consider the issues of legal personality of cyberphysical systems, the basis, content and legal prospects of the concept of "electronic person" was made by Professor O.A. Yastrebov [2]. The team of authors of Financial University is engaged in research of legal regulation of AI for the third year. After analyzing many approaches to creating a legal and regulatory framework, the author's team concluded that it is important to consider the risks and possible negative consequences of using robotic systems and AI [3].

It should be noted that the topic of legal regulation of AI, including the narrow application of this technology in medicine, has been repeatedly raised in foreign scientific literature. Both the broad theoretical issues of the application of AI in various health applications and the more practical and specialized developments, which can be used in the applied activities of medical organizations and in the management of public health bodies.

The problem of integration of modern IT-technologies, as well as technologies using artificial intelligence in the field of health care, is one of the most fascinating and at the same time difficult questions of actual legal theory. The initial postulates for further legal research will be as follows:

- interaction with intelligent systems is possible not as subjects, but as mechanisms, "sources of increased danger";
- final decision and responsibility will be for the person, for the subjects of law (natural or legal persons).

We understand that for artificial intellectual systems such concepts as "human factor", "subjective experiences", "intention", "negligence", "presumption of innocence" and others, practically do not take into account when making decisions. Accordingly, responsibility cannot be shifted from the subject of law (in traditional legal doctrine) to artificial intelligence. The use of artificial intelligence should be embedded in a special legal regime. The institutions of law related to their use should be provided for and regulated in the basic legal acts, are in demand by various branches of law and legislation. Earlier in our research, we formulated conceptual conclusions that should form the basis of further development [3–7]. The issue of health law is particularly acute in the context of the digitalization of health care, where only part of the issue has been developed regarding the safety of medical products using AI technology.

On the other hand, the question arises: how much automated system is "responsible" for decision-making. The subject of administration should be responsible for its actions as its own, because the legal consequences are real, and not "virtually". Incorrect diagnosis of the patient on the basis of the mechanism "telemedicine" should entail the same legal consequences as for actions in the normal environment. Otherwise, we get "fiction of a legal entity" and "fiction of a natural person", "fiction of an official, specialist" etc. Where there is no or incomplete liability in such cases, the very basis of the right, the criteria of permissible and impermissible. "Foreign researchers come to the conclusion that there is a sign of equality between the construction of the legal entity and the autonomous system: the robot can operate the company without any human substrate. This problem goes beyond the study of the possibility of applying the legal entity fiction to such systems" [8, p. 357]. Thus, the actions and decisions of any automated system are equivalent to the activities of the legal entity that administers

it. The publication also deals with the management rights system of the company. The author concludes that it is necessary to improve the corporate legislation in terms of developing a special legal regime to determine the nature of the rights and obligations of the legal entity transferred through the automated system. But there is also a contrary opinion, for example, E. A. Sukhanov believes that the basic definitions in the Civil Code of the Russian Federation are quite applicable for the digital environment and there is no need to allocate digital rights and assets in a special group. This could disrupt the regulation of civil rights objects. Both real and virtual objects of civil rights should have the same legal regulation [9, p. 296]. This approach also deserves attention. This requires extensive legal regulation, enshrined not only at the level of civil legislation, but also specialized medical legislation to detail digital rights, digital objects, etc.

A separate problem is the transmission of data constituting a secret, including medical confidentiality. Who is responsible for the transmission of data by an automated system if the person has not given consent to the transmission and processing of the data? This also raises the question of the reliability of the verification system for electronic signature certificates. "Cybersecurity analysts are doing everything possible — quickly studying new threats, releasing tools to protect against them, which are quickly spread. But the fact remains that between the first attack and the advent of the latest countermeasures, users remain defenseless" [10].

Problems of intellectual property protection are connected with the circulation of objects of intellectual rights on virtual platforms. "The complexity of regulating Internet processes affecting intellectual property rights is primarily due to the extraterritoriality of the Internet environment, which sometimes makes it difficult to define the boundaries of national legislation" [11].

The transition to digital governance should not only remove barriers to entry, ensure equal rights of access to information, but also control the process of using the data transferred to the system by attackers. There are opportunities to transmit distorted information, to anticipate threats and risks of cyberattacks, to ensure the protection of information. In the automatic data interchange system "necessary to legislatively work out the issues of validation of the legal validity and significance of the transmitted digital information. To begin with, a special legal regime must be established and elaborated to take certain actions in the digital economy" [12, p. 114]. These include decentralized registry management, certification of rights and automatic data exchange.

In the Russian Federation, according to V. S. Cherenkova, "for full protection of personal medical data, they should be qualified by the court as medical confidentiality" [13, p. 134].

In the European Union, a broader interpretation of medical personal data, as pointed out in particular by the European Court of Human Rights, which decided, "that the expression "health data" should be interpreted broadly to include information relating to all aspects of both physical and mental health. Analyzing Deal T-343/13 — CN v. Parliament from 3 December 2015, E. B. Luparev notes that this concept cannot be expanded to include provisions that do not lead to the disclosure of any data related to a person's health or medical indications" [14]. The author of the article draws attention to the role of the operator of the information system through which information containing medical confidentiality is exchanged. If the medical service is rendered poor-quality due to the fault of the operator of the information system, he is a subject of civil liability [14].

Worldwide, as Professor I. V. Ponkin argued in 2018, is the problem "virtually no regulatory legal regulation and regulatory technical regulation of the bases, conditions

and features of development, start-up, operation and activity, integration into other systems and monitoring of artificial intelligence technologies" [15, p. 91].

Over the past two years, this problem has been resolved intensively, and numerous regulations have been adopted, which we will elaborate on in this publication.

The main hypothesis of our research results is that AI should not end up being a legal subject in all areas of public relations, including health. It is advisable to classify all actions of automated systems as high-risk facilities for the operation of which subjects of their administration are responsible. However, a special legal regime should be developed that defined the legal consequences of the actions and decisions of intelligent machines, and provided for legal liability. The object of the right should never be a subject of law and should enjoy the rights and protection of such a subject. Neither the presumption of innocence nor other human rights gains, nor the guarantees of rights established by law, must cease to exist. The results of the use of automatic means cannot be initially uncontroversial and accepted without evidence to bring a person to justice, etc. Such practices, as well as other negative decisions on the application and transfer of responsibility to intellectual systems from the standpoint of human rights, violate existing standards and norms of international law.

WHAT MODERN MEDICINE REPRESENTS BASED ON THE USE OF MODERN TECHNOLOGIES, INCLUDING AI?

On the basis of the introduction of information technologies, the formation and development of patient-oriented medicine is being accelerated throughout the world, including in Russia. In order to implement the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030, Strategy for the development of medical science in the Russian Federation for the period up to 2025, a priority project "Improvement of the processes of organization of medical care on the basis of introduction of information technologies", approved by the protocol of the Council under the President of the Russian Federation on strategic development and priority projects from 25 November 2016 No. 9; and Order of the Government of the Russian Federation from 28 July 2017 No. 1632 "Digital Economy of the Russian Federation" (no longer valid); and Decree of the President of the Russian Federation from 21 July 2020 No. 474 "National development objectives of the Russian Federation for the period up to 2030", where one of the national goals is "Digital Transformation", and other documents provides for the development of **patient-oriented medicine** using modern innovative technologies, including information technologies.

Development of legal regulation of patient-oriented medicine and transformation on its basis of the health system is impossible without legal enforcement of artificial intelligence technologies in medicine.

In the Address of the President of the Russian Federation to the Federal Assembly of the Russian Federation dated from March 2018, V. V. Putin noted that "the role, position of the state in the modern world determine not only and not so much natural resources, production capacity, (...) and above all people, conditions for development, self-realization, creativity of each person. Therefore, the basis of everything is the saving of the people of Russia and the well-being of our citizens. This is where we need to make a decisive breakthrough", "in the shortest possible time we need to create an advanced legislative framework, remove all barriers to the development and wide application of robotics, artificial intelligence, unmanned transport, e-commerce, big data processing technologies. And such a regulatory framework should be constantly updated,

based on a flexible approach to each field and technology".[1]

In accordance with the implementation of the President's Address to the Federal Assembly from 20 February 2019, large-scale national level programs in the field of AI have been launched.[2] For example, a national AI strategy was developed in 2019[3] and in the last year or a year and a half a number of other normative legal acts significant for the development of AI technologies in the health system.

According to experts, a modern health system and a traditional approach to treatment cannot be considered effective for a number of reasons, and not only for economic reasons. There is evidence that about half of patients do not have the desired result [16]. Recourse to **patient-oriented** rather than **client-oriented** medicine will be in accordance with the principles of humanism and the values proclaimed by the Constitution of the Russian Federation, human rights and freedoms, foremost among which are the right to life and health.[4] The application of artificial intelligence technologies in patient-oriented medicine is based on interconnection "information technology, clinical therapy, marketing approach, legal support aimed at both improving health and meeting the needs of patients" [16].

Problems of health, its protection and guarantees by the State are the focus of attention of scientists. The search for new socio-innovative approaches based on the principles of evidence-based medicine, to solving the problems of medical care from the perspective of intersectoral interaction between the State, business and civil society becomes the most important national task.

An important aspect of the creation and development of patient-oriented medical information systems is interaction with the professional community. The scientific literature pays some attention to the digitalization of health care. So, individual authors specializing in medicine, reveal the features of patient-oriented medicine [17–22].

Patient-oriented medicine is a medical approach that focuses on the needs of the patient. This requires refocusing and reconfiguring health information systems in accordance with the principles of personalized medicine. Treatment analysis can inform the implementation of information technology by revealing roles, actions and other important data, such as information transfer and situational awareness requirements. Such data can be obtained through electronic workflows, including clinical observations [23] and database analysis [24, 25]. Nevertheless, research on health work processes tends to focus on medical staff — doctors or nurses. These clinician-oriented models often describe a series of discrete actions of a particular type of doctor and the amount of time spent on each type of activity. Less common, but no less important, are patient-oriented studies that describe the sequence of actions of all involved health-care personnel to assist a particular patient [26].

K. Blakemore was working on the assessment the role of the State through the system of medical institutions in the field of client-oriented medicine [27].

The organization of client-oriented medicine is within the scope of attention in the works of L.M. Mukharyamova, I.B. Kuznetsova, G. G. Vafina [28], L. A. Goncharov [29] et al. Authors S. P. Troshin, I. N. Legkova, K.V. Gavrilenko reveal the features of patient-

[1] In the Address of the President of the Russian Federation to the Federal Assembly from 01 March 2018. Rossiyskaya Gazeta. No. 46. 02 March 2018.

[2] In the Address of the President of the Russian Federation to the Federal Assembly from 20 February 2019. Rossiyskaya Gazeta. No. 38. 21 February 2019.

[3] Decree of the President of the Russian Federation from 10 October 2019 No. 490 "On the development of artificial intelligence in the Russian Federation" (with the «National Strategy for the Development of Artificial Intelligence until 2030»). Legislative assembly of the Russian Federation, 14 October 2019, No. 41, art. 5700.

[4] The Constitution of the Russian Federation (adopted by popular vote on 12 December 1993 with the amendments approved by the All-Russian vote on 01 July 2020). Official Internet Legal Information Portal. URL: http://www.pravo.gov.ru, 04 July 2020.

oriented medicine on the basis of the use of modern information technologies [30].

AI technologies are used intensively in health care. Doctors already have medical robots of various types (for example, Da Vinci and Hospice surgical systems). In the field of health, AI technologies are used in disease diagnosis and forecasting, data collection, identification of patients at high risk of disease, drug development. The most promising use of AI in telemedicine and diagnostics [19]. According to some researchers, e-health has become one of the main "drivers" of the entire industry [31].

The improvement of medical care and optimization of health care management are engaged not only directly health institutions, but also many major IT-companies. So, IBM® Watson Health™ proposes three stages in the evolution of the use of information technology in health care:

1) digitization of routine processes in the health and medical care system (for example, MRI, CT scan, automatic management of payment for services, digitalization of data storage, access to their turnover);

2) rejection of old models and applying such breakthrough innovations as artificial intelligence, mobile technology, analytics and cloud[5];

3) transformation of the health-care system, which will integrate and integrate the digital functions and processes of health-care institutions and other organizations in the health-care system.

By implementing the stages of evolution formulated by the company IBM® Watson Health™, healthcare from a technological point of view will turn "from scattered fragments into an integrated ecosystem, allowing the medical professionals to successfully solve problems on a larger scale, keeping the focus on the patient, and provide value-oriented medical care".[6]

The necessity of introduction of AI in the health system is stated in the Strategy of development of the information society in the Russian Federation for 2017–2030,[7] where AI is considered one of the main directions of development of Russian information and communication technologies, along with convergence of communication networks, biotechnologies and cloud computing. According to S. G. Vasin, it is necessary to implement the system of management at the state level using AI [32]. As a confirmation of this thesis, the author cites examples from the National Artificial Intelligence Strategic Plan, from the UK Digital Economy Strategy. These documents give considerable attention to the application of AI in the field of social relations, and also raise issues of public investment in

[5] 1. The cloud provides flexibility and scalability to run and manage a set of analytical capabilities that support current and next-generation applications, all in a secure environment. Ultimately, the cloud analytics platform can share data to potentially help physicians, patients, caregivers and clinicians make timely and effective decisions about patients' treatment. 2. AI has already been used in health care to construct disease-specific progression models and to analyses genetic information to determine treatment effectiveness. AI can also be used for the design and development of clinical trials, previously labor-intensive and manual process. Already now, AI-automated trial matching can integrate data from electronic medical records, medical literature and eligibility criteria from legislators and learn to interpret test requirements based on patient cases. 3. Internet of Things. Using this capability requires a robust and integrated approach that allows multiple micro-services and devices to operate on the same analytical platform. Reduced sensor costs and growth of protected cloud platforms can have a profound impact on the healthcare industry. 4. Blockchain may offer a solution for safe access to health data. The data added to the blockchain can be transmitted almost in real time to a group of authorized persons and/or institutions. Each event or transaction is timed and becomes part of an object's immutable record, be it a drug record or a patient record. The transparency provided by blockchains moves data from individual, isolated ownership to a shared, secure record for permitted stakeholders. This public record becomes the only source of truth for the patient's history (or thing), freely carried by the patient in the form of a digital record, regardless of the location or health system. 5. Quantum will enable quantum computing to identify patterns and obtain information in artificial intelligence systems so complex that the world simply lacks classical computer resources to model them, including drug research and development.

[6] Technologies open the way for health transformation. URL: https://www.ibm.com/ru-ru/watson-health/learn/healthcare-transformation (accessed on 17 March 2021).

[7] Decree of the President of the Russian Federation from 09 May 2017 No. 203 "On the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030". Legislative assembly of the Russian Federation. 2017. No. 20. Art. 2901.

these spheres of public administration. As the author correctly points out, foreign countries have been paying attention to this issue for quite a long time: as an example, the comprehensive report of the National Council for Science and Technology of the USA can be cited "Preparing For the Future of Artificial Intelligence. Executive Office of the President National Science and Technology Council Committee on Technology" for 2016.[8] A significant part of the report is devoted to the need for public investment in the development of AI-solutions in the field of social relations, including health, which should lead to an increase in productivity, reducing working hours, increasing wages, and ultimately the prosperity of American companies and workers, as well as continuing the leadership of the American nation in the creation and use of AI.[9]

When analyzing scientific publications on the current state of digitalization of medicine, business process researchers Sascha Kraus, Francesco Schiavone, Anna Pluzhnikova, Anna Chiara Invernizzi, five main areas of focus in health management: development and introduction of effective medical products using AI; patient-centred approach; organizational factors and improvement of health management; personnel policy; socio-economic aspects [33]. In particular, the authors recommend scientists to address in the future the reliability of solutions using AI technologies in the field of health care.

The direct applicability of information technologies in healthcare was researched by scientists I. C. Marques and J. J. Ferreira. After reviewing the scientific literature on digitalization in the field of health, they propose to highlight seven main directions: 1) integrated information technology management in health care; 2) medical images; 3) electronic health records; 4) information technology and portable devices in health care; 5) access to e-health; 6) telemedicine; 7) medical confidentiality [34].

The collection, processing and circulation of big data is an essential part of the digitalization of health care. They are based on clinical research results, electronic health records (EHR), as well as personal data of patients or users of medical products obtained from self-testing devices, such as wearable devices for monitoring work or sports [35]. Patient records usually include all treatment documentation: written and visual medical records, doctors' letters, e-prescriptions, and insurance payments. Siemens Medical Solutions USA, Inc. considers that the main producers of such data are medical products suppliers, support service providers (e.g., pharmaceutical companies), public and private institutions and patients.[10] In order to establish a legal regime for data trafficking in health care, it is important to define the entire list of entities possessing information that could potentially constitute medical confidentiality.

Big data-based, artificial intelligence-processed analytics will help develop personalized individual help in predictive models for large populations.

The correct use of big health data requires the collection of reliable data, including medical records, genomics and information obtained from various applications.

Electronic Health Cards (EHR) represent the «patient data repository in digital form, secure storage and exchange accessible to many users» [36].

[8] Preparing For the Future of Artificial Intelligence. Executive Office of the President National Science and Technology Council Committee on Technology, October 2016. URL: https://obamawhitehouse.archives.gov/sites/ default/files/ whitehouse_files/microsites/ostp/NSTC/preparing_for_the_ future_of_ai.pdf (accessed on 17.03.2021).

[9] Artificial intelligence, automation, and the economy. Executive Office of the President Washington, D.C. 20502. December 20, 2016. 55 p. URL: https://obamawhitehouse.archives.gov/ sites/whitehouse.gov/files/ documents/Artificial-Intelligence-Automation-Economy.pdf. (accessed on 28.03.2021).

[10] Knight M. Healthcare Dives into Big Data Increasingly used data-driven care protocols will change healthcare delivery systems globally. August 5, 2015. URL: https://www.siemens-healthineers.com/en-us/news-and-events/mso-big-data-and-healthcare-1 (accessed on 28.03.2021).

In addition to EHR, electronic medical records (EMR) are used in the digitization of health care, representing "digital systems that functionally provide patient history, patient demographic data and registration data" for the use of professionals, often based on telemedicine approaches [37]. With EMR systems, it is possible to solve many problems related to the analysis of data in the healthcare system and improvement of operational processes involving AI.

However, not all foreign scientists welcome the concept of digital health care. Some have emphasized that digitalization based on big data, mobile health, e-health, telemedicine and tele-health clearly undermines traditional health systems. A number of scientists cite the destructive trend of further digital transformative technologies, such as artificial intelligence and robotics [38–40].

LEGAL REGULATION

In the EU, a strategy for the development and use of artificial intelligence was adopted in April 2018. From mid-2019, national plans for the development of AI, the creation of funds to finance start-ups for the development of AI technologies were adopted. Financing of the "Digital Europe" program (the duration of the program — from 2021 to 2027) according to the current version approved by the European Parliament and the Council of the European Union, is 9.2 billion euros. Among them, it is planned to allocate 2.7 billion euros for high-performance computing; 2.5 billion euros for artificial intelligence; 2 billion euros to increase cyber security and confidence; 1.3 billion euros to ensure wide use of digital technologies in the economy and society and 700 million euros to develop digital skills.

The European Parliament Resolution on Comprehensive European Industrial Policy on AI and Robotics, published in February 2019, establishes general provisions of a recommendatory nature. For example, the resolution contains recommendations on the application of AI technologies in the field of health.

A digital platform has been established by the joint task force from ITU (International Telecommunication Union) and WHO (World Health Organization) on AI for Health (FG-A14H) to test and compare AI applications for health.[11] The task force itself includes experts and representatives of stakeholders in the field of research, practice, ethics and legal regulation in health, capable of developing guidance documents related to ethics, evaluation, legal regulation of AI for application in various fields of health care — in ophthalmology, histopathology, dentistry, radiology, etc. All documentation of this group is publicly available.

The EU Ethics Guide for AI is an important tool for the application of AI technologies in different areas of society. The management has established a common three AI principles that can be summed up as doing well, doing no harm, and operating transparently. These principles are expected to lead to sustainable development of AI technologies: they must be safe, accountable, non-discriminatory, and human.

These EU documents are, in fact, the basic legal basis for the legal regulation of AI in the field of health care. Many developed States have rules for the collection of patient data. These include the Health Insurance Portability and Accountability Act (HIPPA) and the European General Data Protection Regulation (GDPR). In the US, HIPPA also protects patients' medical data. Such data collection is necessary for machine learning and the use of AI in health care.

The proposed path of legal regulation development in the EU states is reasonable, but does not take into account the risks arising from such activities [41]. Insurance is one way to cover health risks and to recover costs for medical care. The Federal Republic of Germany adopted the German Digital Health Act in November 2019 (Digitale

[11] ITU-WHO Task Force on Artificial Intelligence. URL: https://ru.abcdef.wiki/wiki/ITU-WHO_Focus_Group_on_Artificial_Intelligence_for_Health (accessed on 28.03.2021).

Versorgung Gesetz — DVG), which entitles all persons covered by statutory health insurance to reimbursement for certain digital medical applications (i.e. insurers will pay for their use).[12] It is known that the German compulsory health insurance system is one of the largest in the world. Approximately 90% of the population (about 75 million people) in Germany is covered by public health insurance and the remaining 10% by private insurance. The DVG (Digital Health Care) Act entitles those who are insured by an independent provider of compulsory health insurance in Germany to receive insurance payments for certain digital medical applications.

As a rule, insured persons are entitled to insurance payments on digital medical applications if they meet the following criteria:

1. Are medical products with lower risk.

2. Their main function is based on digital technology.

3. They are designed to support the monitoring, detection, relief or treatment of diseases, injuries, care provided by service providers.

4. They were included in the newly established official register of digital medical applications maintained by the Federal Institute of Medicines and Medical Products of Germany (Bundesinstitut für Arzneimittel und Medizinprodukte — BfArM).

5. They are used either with the consent of the medical insurer or by appointment of the attending physician or psychotherapist [SGB V, § 33a(1)].

In addition, DVG also aims to accelerate the introduction and use of telemedicine. In particular, within the framework of DVG the patient can easily take advantage of video consultations. During such consultation, the patient may be informed of the circumstances essential to consent to medical care, including its nature, scope, implementation, anticipated risks and consequences (SGB V, § 291g (4); BGB 14, § 630e). DVG also contains provisions to make demographic data from health insurers more suitable for research purposes (SGB V, § § 303a-303f). In particular, under the General Data Protection Regulation 2016/679 (GDPR), DVG allows certain beneficiaries, such as universities and publicly funded research institutions (e.g., the Max Planck Society) are process certain demographic data from health insurers for specific research purposes, especially for the analysis of treatment or care processes over longer periods (SGB V, § § 303b, 303e(1) and (2).

In the US, the federal Medicare Program provides coverage for more than 60 million Americans.[13] Since 2019, Medicare Part B (outpatient health insurance) provides insurance coverage for some telemedicine services such as office visits, psychotherapy and other consultations. In 2020, during the COVID-19 pandemic, Medicare significantly expanded its telemedicine coverage policy.

Health insurance, which stimulates the accelerated adoption of AI technologies, provides both Germany and the US with cost recovery for innovative technologies and useful digital health solutions.

Over 318,000 mobile health apps are available worldwide, and about 200 apps are added to app stores every day [42].

Researchers of the problems of legal regulation of digitalization of healthcare Sara Gerke, Ariel D. Stern and Timo Minssen come to quite legitimate conclusions about the importance of ensuring the safety of patients and consumers when using medical applications. In doing so, safety, functionality, quality, data protection, data security and positive impact on care should be the criteria for their evaluation. The authors of the article thought, «risk-oriented approach can serve as a useful starting point for the development of

[12] Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale-Versorgung-Gesetz — DVG) [Digital Healthcare Act] of 9 December, BGBl I at 2562 (Germany, 2019).

[13] CMS. CMS fast facts. URL: https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/CMS-Fast-Facts/index (2020).

standardized, evidence-based assessment processes and legal requirements for digital health solutions. However, legislative bodies will also need to ensure that they do not over-regulate the sector in a way that would make it too burdensome for producers to comply with qualification requirements and to recover losses, thereby preventing or slowing down innovation» [43].

Independent direction of legal provision of application of AI technologies in the field of health care is development of mandatory requirements for medical products (medical devices). Unlike the development of drugs that are considered dangerous until proven otherwise, the development of medical products should be based on compliance with certain risk requirements.[14] For example, in the United States, the Food and Drug Administration is the regulator of medical products (FDA). The FDA Department of Industry and Consumer Education (DICE) determines whether a digital «device» is a medical product or a product intended for recreational purposes.[15] Medical products can presumably be classified according to the risk profile currently defined by the FDA as Class I, II or III in order of increasing risk. Class I devices require little security testing. Today, about 50% of medical products fall into this category and 95% of them are exempt from the regulatory process.[16]

There are international organizations to streamline the standardization of medical products in digital health care. For example, the Society of Digital Medicine develops a resource on its website (www.dimesociety.org) to track and monitor various standards, documents and requirements.[17]

In a review article "Digital Medicine: A Measurement Textbook", the authors reveal three basic principles of biomedical ethics, as described in the Belmont Report (1978),[18] which are applicable for research of digital technologies:

1. Respect for the individual. This principle is demonstrated through an informed consent process that occurs when a person is given the information necessary to make an informed decision on whether to volunteer. How this information is communicated is important because voluntary participation in the study differs from, say, accepting the Terms of Service (ToS) for accessing the application or signing the consent form for receiving medical care.

2. Charity. This is when the assessment of the likelihood and magnitude of potential harm is compared with the possible benefits to the participant, the people it represents and society.

3. Equity. This principle focuses on the equitable sharing of the benefits and burdens of research and development [44].

In scientific articles on digitalization of health care authors pay attention to the problems of information security and protection of information, both personal and personal medical information.

Healthcare has witnessed the spread of vulnerabilities, especially in related technologies, many of which are vital: Johnson & Johnson insulin pumps, implantable St. Jude Medical heart devices, and WannaCry extortion attacks, which infected 200 000 computers, many of which

[14] U.S. Food and Drug Administration. Information Sheet Guidance For IRBs, Clinical Investigators, and Sponsors. Silver Spring, MD: U.S. Food and Drug Administration. January 2006. 15 p. URL: https://www.fda.gov/downloads/RegulatoryInformation/Guidances/UCM126418.pdf (accessed on 28.03.2021).

[15] U.S. Food and Drug Administration. Multiple Function Device Products. Policy and Considerations. Silver Spring: U.S. Food and Drug Administration. 2018 Apr 27. 18 p. URL: https://www.fda.gov/ucm/groups/fdagov-public/@fdagov-meddev-gen/documents/document/ucm605683.pdf (accessed on 28.03.2021).

[16] U.S. Food and Drug Administration. Reclassification [Internet] [updated 2018 Dec 13]. URL: https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm080412.htm (accessed on 28.03.2021).

[17] The Digital Medicine Society. The Digital Medicine (DiMe) Society. 2019. URL: www.dimesociety.org (accessed on 28.03.2021).

[18] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, Department of Health, Education and Welfare (DHEW). The Belmont Report. Washington: United States Government Printing Office. 1978 September 30. URL: https://videocast.nih.gov/pdf/ohrp_belmont_report.pdf (accessed on 28.03.2021).

are part of the critical infrastructure of hospitals, in 150 countries [45].

In addition to hacking attacks, medical professionals can also illegally disseminate information. A number of researchers developed the project "Hippocratic oaths for connected medical devices" (HOCMD).[19] The Oath sets out a number of principles of safety and ethics, including "safety by design" and "sustainability and containment" [46].

Describing the issues of the use of AI in healthcare and its legal regulation in the Russian Federation, it is necessary to mention the national project «Healthcare», which identified the key task of digitalization of the healthcare system.[20] Within the framework of the project, the federal project "Creation of a unified digital circuit in health care on the basis of the unified state information system in the field of health care was adopted (USHIS)",[21] which will categorize all health organizations with information systems, information and telecommunication networks, automated management systems as critical information infrastructure (KII).[22] Will be subject to categorization AI, ITS, ICS, which provide management, technological, production, financial-economic and (or) other critical business processes within the framework of the performance of functions (powers) or the implementation of activities of a health organization. As a result, a list of potentially significant KII facilities for health care organizations will be established and a single digital circuit in health care will be created based on a unified State information system in the health sector (USHIS). The overall objective of digitalization is to ensure that reliable and structured information is readily available to doctors and managers.

For citizens, the main patient-oriented service is "My Health", allowing you to make an appointment with a doctor; attach to a medical organization; submit an application on the choice of an insurance medical organization; to obtain information on the provided medical services and their cost; to obtain a number of documents, for example, a medical certificate on admission to the driving vehicle, electronic prescriptions, a certificate of vaccination from COVID-19, etc. The service is actively developing.

With the completion of the formation of the Unified State Health Information System (USHIS) within the next four years, electronic patient records Central Medical Imaging Archives and Unified Laboratory Systems to be accessible to all medical institutions in the country. All state medical institutions will be required to provide citizens with access to their electronic medical documents through the Single Portal of State Services.

Telemedicine is being actively developed to make medicine accessible to the geography of our country,[23] which implemented by many health organizations.[24]

Russia is actively working to standardize the use of AI in the field of health care. Thus, in 2020, the first draft of a national

[19] I Am the Cavalry. Hippocratic Oath for Connected Medical Devices. URL: https://www.iamthecavalry.org/domains/medical/oath/ (accessed on 28.03.2021).

[20] Passport of the national project "Healthcare" (approved by the Presidium of the Council under the President of the Russian Federation on strategic development and national projects, protocol of 24.12.2018 No. 16). The document was not published (ConsultantPluse).

[21] National project "Healthcare". The federal project "Creation of a unified digital circuit in healthcare on the basis of the unified state information system in healthcare sphere (USHIS)". Methodological recommendations for the categorization of critical health information infrastructure facilities (Version 1.0) (approved by the Ministry of Health of Russia 05 April 2021). The document was not published (ConsultantPluse).

[22] Federal Law from 26 July 2017 No. 187 "On the Security of the Critical Information Infrastructure of the Russian Federation", 31.07.2017, No. 31 (Part I), art. 4736.

[23] Order of the Ministry of Health of the Russian Federation from 30.11.2017 No. 965 "On approval of the procedure of organization and provision of medical assistance with the use of telemedicine technologies". Official Internet Legal Information Portal. URL: http://www.pravo.gov.ru, 10.01.2018 (accessed on 28.03.2021).

[24] It should be noted that, according to the law on telemedicine, a physician was not entitled to make any recommendations without an initial appointment, and remote diagnosis was prohibited. There are no admission restrictions.

standard for AI in healthcare in Russia was developed, which regulates the conduct of clinical trials of medical AI-systems (AIS). In order to coordinate the work on unification and standardization of requirements for AI systems in healthcare, as well as the establishment of certification requirements for medical products, a subcommittee "Artificial Intelligence in Healthcare" was established as part of TC 164 (PC 01/TC 164).[25]

In accordance with the long-term work plan of the Technical Committee for Standardization "Artificial Intelligence" (TC 164), created on the basis of the Joint-Stock Company "Russian Venture Company" (RVC), by 2027, it is planned to develop about 50 standards in the field of AI in health care in individual areas, including general requirements and classification of AI systems in clinical medicine, big data in health care, functional diagnostics, radiation diagnostics, remote monitoring systems, histology, medical decision support systems, image reconstruction in diagnosis and treatment, medical systems of analysis and forecasting, as well as educational programs in health care.

A task force of the International Organization for Standardization Technical Committee No. 215 "Informatization of Health" has been established to develop standards at the international level (ISO) — TC 215 ISO Health informatics. Its task is to form the requirements to confirm the compliance of high-tech AI systems for their application in health care. In particular, risk assessment of the impact on the health of patients, determination of consistency of medical databases, correctness of withdrawal of decisions and organization of information exchange between AI systems and electronic medical cards, medical products and health information systems.

Based on the analysis provided, it follows that the Russian Federation is actively working on the digitalization of health care, standardizing the use of AI, domestic experts are involved in a number of international organizations, including: the digitalization of health care, there is an exchange of experience both within the state, and with foreign colleagues, telemedicine is being actively developed, AI technologies are being introduced into the high-tech medical care sector, and a single health information circuit is being created in the country on the basis of USHIS.

Taking into account the analysis of the existing legal regulation in Russia and abroad, we propose to build the institutional-legal model of the development of patient-oriented medicine on the basis of the use of AI as follows.

1. The model is based on a paradigm shift from client-oriented to patient- oriented medicine.

2. The main elements of the model are:

- digitalization of management processes in the health system (management of medical services, digitization of the formation and circulation of medical data, digitization of the organization's access to them, electronic medical cards, electronic medical records);
- digitization of medical care (e.g., MRI, CT, high-tech robotic operations, database creation and turnover);
- integration processes in the health care system, unification of digital functions of management of medical institutions and digital processes of organization and provision of medical care and medical services in a unified system of health organizations, independently of organizational andlegal forms of specific medical and pharmaceutical institutions;
- development of mandatory requirements for medical products (medical devices) using risk-based AI and their implementation through pilot legal regimes (regulatory sandboxes). The legal framework

[25] Order of Rosstandart from 31 December 2019 No. 3471 «On making amendments to the order of the Federal Agency for Technical Regulation and Metrology from 25 July 2019 No. 1732 «On creation of technical committee for standardization Artificial Intelligence». The document was not published. ConsultantPluse.

for their regulation is the basic AI principles applicable, inter alia, in the field of health;

• intensive spatial development of telemedicine, especially in hard-to-reach areas of our country;

• introduction and promotion of the institution of self-regulation of medical ethics, including the observance of medical confidentiality in the context of the digitization of medical care and medical services;

• Introduction of a financial and legal mechanism for the use of AI in the health-care system, the basis of which should be the institute of health insurance by including in the list of insurance coverage under the CHI the provision of medical care using AI, provision of telemedicine services, etc.;

• at the international level, the Russian Federation should be represented and participate more actively in the work of international organizations dealing with digital health development.

CONCLUSION

1. The article offers an institutional-legal model of development of patient-oriented medicine based on use of innovative technologies, including AI technologies. Rapid changes are taking place in the health-care system based on technologies that need to be managed in a systemic manner. In this approach, separate rules of different branches of law, together with standards (technical regulation), are considered in close connection with each other.

2. It was found that despite the complexity of forecasting the problems and consequences caused by the use of AI technologies in the field of health, scientific publications highlight the following problems of legal regulation:

• problems with the correct determination of legal responsibility for acts committed using artificial intelligence technologies [1–7, 15];

• problems associated with adapting the newly created norms of law aimed at regulating relations in this sphere to the general body of existing legislation [1, 5];

• problems of ensuring the confidentiality of personal information and personal information in the context of the collection and storage of a large amount of personal information in electronic and automated databases (institute of medical confidentiality);

• problems of standardization of AI technologies in medicine;

• problems of licensing medical products using AI technologies;

• financial and legal problems of providing medical services in digital format.

3. Development of legal regulation of AI in the field of health should be carried out in the following main directions:

– depending on the work performed, the services provided in the digital health system and the high-tech products manufactured for medicine (medical products) and pharmacology;

– depending on the application of weak or strong AI in digital health care;

– depending on the risks and regulatory requirements of cybersecurity, information security, cyberphysical systems security;

– depending on the financing of the work performed, the services provided in the digital health system and the high-tech products manufactured for medicine (medical products) and pharmacology (Stimulation of the State, improvement of the legal mechanism for payment of medical services and provision of medical assistance using AI technologies through insurance companies).

4. Foreign experience of developed countries (Germany and the United States) demonstrates that legal regulation of digital medicine significantly ahead of domestic in a number of areas. In particular, the institution of compulsory health insurance needs to be activated more actively in order to foster innovation in the health system.

It is also a positive experience to develop the bioethical principles needed to engage citizens as volunteers in medical research.

It is appropriate for the medical community at the level of self-regulation of medical ethics to modernize the "Hippocratic Oath" for the digital healthcare environment.

5. International standardization and domestic technical standardization demonstrate the approach to technical regulation of medical products as narrow profile. This approach should be evaluated positively. So, in 2020–2021, numerous domestic standards have been adopted in the form of GOSTs and preliminary GOSTs establishing terminology and safety requirements. This unquestionably regulates the requirements for AI technologies in digital healthcare.

The second big part of the legal regulation in the field of technical regulation is special standards in medicine, mainly for certain medical products. In addition, requires improvement and the institute of licensing of medical products (separation with household goods in the field of health), accelerated introduction of innovative technologies AI, robotics, CPS, work in medicine, used in finished products or in the provision of health services and works. Finished products require more careful control and supervision by the State. In particular, in addition to compliance with standards, medical products are subject to compulsory licensing (this is the cost, effort and most importantly — time).

6. It is proposed to apply more regulatory sandboxes — experimental legal regimes for the following chain: new technologies — high-tech medicine — experimental treatments.

ACKNOWLEDGEMENTS

The article is based on the results of the III stage of the basic research work of the University of Finance on "The theory of legal regulation of artificial intelligence, robots and robotics objects in the Russian Federation". Financial University, Moscow, Russia.

REFERENCES

1. Morkhat P.M. Artificial intelligence: Legal view. Moscow: Buki Vedi; 2017. 257 p. (In Russ.).
2. Yastrebov O.A. Discussion about the prerequisites for assigning robots the legal status of "electronic persons". *Voprosy pravovedeniya*. 2017;(1):189–202. (In Russ.).
3. Ruchkina G.F., ed. The theory of legal regulation of artificial intelligence, robots and robotics objects in the Russian Federation. Moscow: Prometheus; 2020. 296 p. (In Russ.).
4. Popova A.V. Legal aspects of artificial intelligence ontology. *Gosudarstvo i pravo = State and Law*. 2020;(11):115–127. (In Russ.). DOI: 10.31857/S 102694520012531–5
5. Popova A.V. Ethical principles of interaction with artificial intelligence as a basis of legal regulation. *Pravovoe gosudarstvo: teoriya i praktika = The Rule of Law State: Theory and Practice*. 2020;(3):34–43. (In Russ.). DOI: 10.33184/pravgos-2020.3.4
6. Gorokhova S.S. Artificial intelligence-based technologies: Prospects and liability in the legal environment. *Yurist = Jurist*. 2021;(6):60–67. (In Russ.). DOI: 10.18572/1812–3929–2021–6–60–67
7. Sviridova E.A., Rahmatulina R.S., Shaydullina V.K., Gorohova S.S., Lapina M.A. Issues of economic and legal responsibility in the application of artificial intelligence technologies in the coal industry. *Ugol'*. 2020;(7):57–61. (In Russ.). DOI: 10.18796/0041–5790–2020–7–57–61
8. Serova O.A. Problems of development of the methodology of civil law research in the digital age. *Metodologicheskie problemy tsivilisticheskikh issledovanii = Methodological Problems of the Civil Law Researches*. 2019;1(1):351–362. (In Russ.).
9. Vaipan V.A., Egorova M.A., eds. Legal regulation of economic relations in modern conditions of digital economy development. Moscow: Yustitsinform; 2019. 376 p. (In Russ.).
10. Gnidenko I.G., Egorova I.V., Merdina O.D. Intelligent systems as a vector of enterprise information security development. *Peterburgskii ekonomicheskii zhurnal = Saint-Petersburg Economic Journal*. 2020;(1):147–154. (In Russ.). DOI: 10.25631/PEJ.2020.1.147.154

11. Elchaninova N.B. The problems of legal protection of intellectual property on the Internet. *Obshchestvo: politika, ekonomika, pravo = Society: Politics, Economics, Law*. 2016;(12):118–120. (In Russ.).
12. Ruchkina G.F., Lapina M.A., eds. Public-legal means of economic and financial development efficiency. Pt. 1. Public-legal means of digitalization of management, economic and social space. Moscow: RuScience; 2020. 246 p. (In Russ.).
13. Lazarev V.V., Gadzhiev Kh.I., Alimov E.V. et al. Data protection: Scientific and practical comment on judicial practice. Moscow: Kontrakt; 2020. 176 p. (In Russ.).
14. Luparev E.B. Legal regulation of the export of telemedicine services: Russian and European experience. *Kubanskoe agentstvo sudebnoi informatsii PRO-SUD-123.RU: Yuridicheskii setevoi elektronnyi nauchnyi zhurnal*. 2020;(1):69–78. (In Russ.).
15. Ponkin I.V., Redkina A.I. Artificial intelligence from the point of view of law. *Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Yuridicheskie nauki = RUDN Journal of Law*. 2018;22(1):91–109. (In Russ.). DOI: 10.22363/2313–2337–2018–22–1–91–109
16. Dudnik V. Yu. A model of personalized medical care. *Akademicheskii zhurnal Zapadnoi Sibiri = Academic Journal of West Siberia*. 2016;12(1):98–100. (In Russ.).
17. Nikolaev N. Patient-oriented antihypertensive therapy: Clinical guidelines for practitioner. *Vrach = The Doctor*. 2016;(4):82–85. (In Russ.).
18. Menshikov A.N. Development of a model of patient-oriented healthcare in the Republic of Bashkortostan. *Obyazatel'noe meditsinskoe strakhovanie v Rossiiskoi Federatsii*. 2016;(3):34–37. (In Russ.).
19. Troshin S.P., Legkova I.N., Gavrilenko K.V. Creation of a patient-oriented models of obligatory medical insurance based on the application of current information technologies. *Obyazatel'noe meditsinskoe strakhovanie v Rossiiskoi Federatsii*. 2016;(6):34–41. (In Russ.).
20. Averin A.V., Shvardakova O.A. Patient-oriented technologies in the practice of a multidisciplinary medical organization. *Glavnaya meditsinskaya sestra*. 2015;(10):39–48. (In Russ.).
21. Kitaeva E.A., Kitaev M.R., Suetina T.A., Salyahova L. Ya., Vafin A. Yu. Implementation of patient oriented program aiming to develop compliance to drug therapy in rural area patients (in terms of Rybnaya Sloboda district of the Republic of Tatarstan). *Vestnik sovremennoi klinicheskoi meditsiny = The Bulletin of Contemporary Clinical Medicine*. 2017;10(2):64–71. DOI: 10.20969/VSKM.2017.10(2).64–71
22. Schunk M., Stark R., Reitmeir P., Meisinger C., Holle R. Towards patient-oriented diabetes care: Results from two KORA surveys in Southern Germany. *Journal of Diabetes Research*. 2015;2015:368570. DOI: 10.1155/2015/368570
23. Zheng K., Haftel H.M., Hirschl R.B., O'Reilly M., Hanauer D.A. Quantifying the impact of health IT implementations on clinical workflow: A new methodological perspective. *Journal of the American Medical Informatics Association*. 2010;17(4):454–461. DOI: 10.1136/jamia.2010.004440
24. Huang Z., Lu X., Duan H. On mining clinical pathway patterns from medical behaviors. *Artificial Intelligence in Medicine*. 2012;56(1):35–50. DOI: 10.1016/j.artmed.2012.06.002
25. Bouarfa L., Dankelman J. Workflow mining and outlier detection from clinical activity logs. *Journal of Biomedical Informatics*. 2012;45(6):1185–1190. DOI: 10.1016/j.jbi.2012.08.003
26. Ozkaynak M. Characterizing workflow in hospital emergency departments. Madison, WI: University of Wisconsin-Madison; 2011.
27. Blakemore K. Are professionals good for you? The example of health policy and health professionals. In: Blakemore K. Social policy: An introduction. Buckingham, Philadelphia: Open University Press; 1998.
28. Mukharyamova L.M., Kuznetsova I.B., Vafina G.G. Sick, patient, client: The positions of labor migrants in the Russian health care system (evidence from the Republic of Tatarstan). *Vestnik sovremennoi klinicheskoi meditsiny = The Bulletin of Contemporary Clinical Medicine*. 2014;7(1):43–49. (In Russ.).
29. Goncharov L.A. From state paternalism to client orientation? Russian government institutions in search of effective models for the formation and training of the corps of state civil servants. *Vestnik Voronezhskogo instituta ekonomiki i sotsial'nogo upravleniya*. 2017;(2):68–74. (In Russ.).

30. Ponkin I. V., Ponkina A. A., Laptev V. S. Concept of digital public health and e-health. *Narkologiya = Narcology*. 2014;13(6):34–40. (In Russ.).
31. Grishchenko G. A. Artificial intelligence in public administration. *Rossiiskii yuridicheskii zhurnal = Russian Juridical Journal*. 2018;(6):27–31. (In Russ.).
32. Vasin S. G. Artificial intelligence in state management. *Upravlenie*. 2017;5(3):5–10. (In Russ.).
33. Kraus S., Schiavone F., Pluzhnikova A., Invernizzi A. C. Digital transformation in healthcare: Analyzing the current state-of-research. *Journal of Business Research*. 2021;123:557–567. DOI: 10.1016/j.jbusres.2020.10.030
34. Marques I. C.P., Ferreira J. J.M. Digital transformation in the area of health: systematic review of 45 years of evolution. *Health and Technology*. 2020;10(3):575–586. DOI: 10.1007/s12553–019–00402–8
35. North K., Maier R., Haas O., eds. Knowledge management in digital change. Cham: Springer-Verlag; 2018. 394 p. (Progress in IS). DOI: 10.1007/978–3–319–73546–7
36. Häyrinen K., Saranto K., Nykänen P. Definition, structure, content, use and impacts of electronic health records: A review of the research literature. *International Journal of Medical Informatics*. 2008;77(5):291–304. DOI: 10.1016/j.ijmedinf.2007.09.001
37. Chakravorty T., Jha K., Barthwal S. Digital technologies as enablers of care-quality and performance: A conceptual review of hospital supply chain network. *IUP Journal of Supply Chain Management*. 2018;15(3):7–25.
38. Agnihothri S., Cui L., Delasay M., Rajan B. The value of mHealth for managing chronic conditions. *Health Care Management Science*. 2020;23(2):185–202. DOI: 10.1007/s10729–018–9458–2
39. Patrício L., Teixeira J. G., Vink J. A service design approach to healthcare innovation: From decision-making to sense-making and institutional change. *AMS Review*. 2019;9(8):115–120. DOI: 10.1007/s13162–019–00138–8
40. Yousaf K., Mehmood Z., Awan I. A., Saba T., Alharbey R., Qadah T., Alrige M. A. A comprehensive study of mobile-health based assistive technology for the healthcare of dementia and Alzheimer's disease (AD). *Health Care Management Science*. 2020;23(2):287–309. DOI: 10.1007/s10729–019–09486–0
41. Lapina M. A. Theoretical and legal aspects of risk management. *Gosudarstvo i pravo = State and Law*. 2015;(2):35–44. (In Russ.).
42. The rise of mHealth apps: A market snapshot. Liquid State. Mar. 26, 2018. URL: https://liquid-state.com/mhealth-apps-market-snapshot/
43. Gerke S., Stern A. D., Minssen T. Germany's digital health reforms in the COVID-19 era: Lessons and opportunities for other countries. *npj Digital Medicine*. 2020;3(1):94. DOI: 10.1038/s41746–020–0306–7
44. Coravos A., Goldsack J. C., Karlin D. R., Nebeker C., Perakslis E., Zimmerman N., Erb M. K. Digital medicine: A primer on measurement. *Digital Biomarkers*. 2019;3:31–71. DOI: 10.1159/000500413
45. Brewster T. Medical devices hit by ransomware for the first time in US hospitals. Forbes. May 17, 2017. URL: https://www.forbes.com/sites/thomasbrewster/2017/05/17/wannacry-ransomware-hit-real-medical-devices/#dad2b18425cf
46. Woods B., Coravos A., Corman J. D. The case for a Hippocratic Oath for connected medical devices: Viewpoint. *Journal of Medical Internet Research*. 2019;21(3):e12568. DOI: 10.2196/12568

ABOUT THE AUTHOR

Marina A. Lapina — Dr. Sci. (Law.), Professor, Chief Researcher, Professor, Department of International and Public Law, Financial University, Moscow, Russia
https://orcid.org/0000-0003-0320-161X
MALapina@fa.ru

Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

The article was submitted on 02.09.2021; revised on 20.09.2021 and accepted for publication on 27.12.2021.
The author read and approved the final version of the manuscript.