National Research University
Higher School of Economics

Copyright manuscript

Zhuravlev Mikhail Sergeevich

LEGAL ASPECTS OF INFORMATION SECURITY IN TELEMEDICINE

12.00.13 – Information Law

PhD Dissertation Summary for the purpose of obtaining
academic degree Doctor of Philosophy in Law

Academic supervisor:
Bogdanovskaya Irina Yurevna,
Doctor of Science, professor

MOSCOW – 2021

The thesis was completed at the International Laboratory for Information Technology and Intellectual Property Law of the National Research University "Higher School of Economics".

The text of the thesis is deposited and available on the website of the Higher School of Economics: https://www.hse.ru/sci/diss/

Relevance of the research

Many spheres of public life are undergoing changes in the information society and medicine is not an exception. Modern information technologies allow doctors to provide remote medical assistance and monitor the health status of patients. During the COVID-19 pandemic, the need for remote medical care has increased[1]. Machine learning technologies are used to conduct research and detect diseases on the base of automated processing of large amounts of medical data[2]. The spread of telemedicine technologies affects the management in healthcare system, transforms the medical services market and involves new participants in the healthcare economy - owners of telemedicine platforms, telecom operators, cloud service providers, manufacturers of telemedicine devices and software developers[3]. These transformative processes in medicine require adequate mechanisms of legal regulation that specify the legal status of the telemedicine participants, protect the rights of patients and public interests in the field of healthcare.

In the context of medicine digitalization, the importance of information security of patients and other healthcare participants is increasing. Processing large volumes of health personal data in information systems increases the risks of privacy violation and requires higher standards of data protection. On the other hand, legal mechanisms are needed to ensure access to medical data and reliable document exchange between participants of telemedicine relations[4].

Information security in telemedicine, first of all, is ensured by guarantees of the patients' information rights: the patient's right to privacy and personal data

---

[1] Telemeditsinskiye tekhnologii poluchili vo vremya pandemii stimul k razvitiyu. Rossiyskaya gazeta. Special issue No. 237 (8291) [Electronic resource] URL: https://rg.ru/2020/10/21/pandemiia-prostimulirovala-razvitie-telemedicinskih-tehnologij.html (date of access: 01.02.2021).

[2] Bursov A.I. The use of artificial intelligence for the analysis of medical data // Almanac of Clinical Medicine. 2019. No. 7. [Electronic resource] URL: https://cyberleninka.ru/article/n/primenenie-iskusstvennogo-intellekta-dlya-analiza-meditsinskih-dannyh (date of access: 01.02.2021).

[3] Digital transformation and interoperability. 2020 Global Health Care Outlook. P. 19 [Electronic resource] URL: https://documents.deloitte.com/insights/2020globalhealthcareoutlook (date accessed: 02/01/2021).

[4] A 2017 European Commission study identifies privacy risks, cyber threats and underdeveloped infrastructure as the main barriers to accessing health data. Synopsis report of the public consultation on Digital transformation of health and care in the context of the Digital Single Market [Electronic resource] URL: https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-digital-transformation-health-and-care-context-digital (date of access: 02/01/2021).

protection; the patient's right to access information about his health status. Currently, Russian law has not developed a uniform approach to the creation and circulation of electronic health records (EHR), unreasonably restricts methods of identification and authentication. Russian legislation does not regulate the provision of anonymous medical care using telemedicine technologies. There are collisions in the requirements for the protection of personal data and provisions on medical secrecy that impede the exercise of patients` rights in telemedicine.

Legal support of information security in telemedicine also covers the protection of public and third parties` interests in access to health data. Protection of public interests in healthcare (management of the healthcare system, protecting the health of other citizens, conducting medical research, etc.) conflicts with the requirements of personal data legislation that predetermines the need to search for new approaches to the legal regulation in the area of health personal data processing[5].

The degree of scientific elaboration and theoretical base of the research

Currently, both in Russian and foreign legal science, there is a high interest in the study of the legal aspects of telemedicine, including information security issues, which is confirmed by a significant number of scientific publications in this area in recent years[6].

---

[5] In legal doctrine this problem is called "privacy - public health dilemma", its importance has increased in the context of the COVID-19 pandemic. See Privacy, security, and public health in a pandemic year [Electronic resource] // URL: https://www.mckinsey.com/business-functions/risk/our-insights/privacy-security-and-public-health -in-a-pandemic-year (date accessed: 02/01/2021).

[6] Until 2016, a small number of works devoted to the legal regulation of telemedicine were presented in the Russian legal literature: V.B. Naumov, D.A. Saveliev. Legal aspects of telemedicine. Saint Petersburg: Anatolia, 2002.107 p.; Bogdanovskaya I.Yu. Legal regulation of telemedicine: the US experience // Physician and Information Technologies, 2007, N 3. pp. 64-68; Shtykova N.N. The essence and problems of the implementation of e-medicine (on the example of the Vladimir region) // Medical Law. 2014. pp. 22-27. However, in the past few years, after the adoption of legislation on telemedicine technologies, telemedicine issues have begun to receive more attention in the domestic legal literature. See, for example, M.S. Varyushin. Legal regulation of telemedicine in Russia and the EU: two steps forward and one back // Zakon. 2018. N 1. pp. 165-174; Smirnova K.M. The problem of information security in the context of using the "Internet of things" in medicine // Medical Law. 2019. N 1. pp. 31-37; Smyshlyaev A.V., Melnikov Yu.Yu., Platonova N.I. Telemedicine technologies in the system of primary health care in the Russian Federation at the present stage: legal aspect // Medical law. 2018. N 6. pp. 16-21; Pospelova S.I., Sergeev Yu.D., Pavlova Yu.V., Kamenskaya N.A. Legal regime for the use of telemedicine technologies and the introduction of electronic document management: the current state of legal regulation and development prospects // Medical Law. 2018. N 5. pp. 24-33; Sokolenko N.N., Bagnyuk M.E., Bagnyuk D.V. Provision of medical care using telemedicine technologies: some problems of legal regulation // Medical Law. 2018.

The theoretical basis of this research includes academic works of Russian and foreign scientists in the area of information law and other branches of law.

Works of Russian scientists in the field of information law played a key role in the theoretical understanding of legal support of information security in telemedicine. The works of I.L. Bachilo, P.U. Kuznetsova, A.B. Agapova, I.M. Rassolova, A.V. Lysenko served as the basis for the study of general issues of information law and information legal relations. Books, research articles and dissertations by T.A. Polyakova, V.N. Lopatina, A.V. Morozov, A.K. Zharova, E.K. Volchinskaya, A.S. Zharova, A.A. Chebotareva, A.A. Streltsov systematically highlighted the theoretical and legal problems of ensuring information security. In the works of A.A. Tedeev, E.V. Semizorov, R.V. Amelin, S.I. Semiletov, M.V. Borodin the legal issues of information systems and electronic document management are disclosed. L.K. Tereshchenko, A.V. Minbaleeva, G.G. Kamalova, V.A. Severin, N.I. Petrykina formed scientific concepts on the legal nature of information and its legal regime. E.V. Talapina, V.B. Naumov, A.I. Saveliev, V.V. Arkhipov, Yu. S. Kharitonova, A.V. Tulikov contributed to the study of evolution of human rights and legal institutions in the post-industrial era.

Telemedicine today belongs to the key research subjects of the leading international IT law centers. In recent years, foreign scientists have carried out a significant amount of research[7] on the protection of personal data in ehealth, on legal status of electronic health records, ensuring the safety of medical devices, creating institutional and infrastructural conditions for the development of telemedicine.

N 4. pp. 14-17; Smirnova K.M. The problem of information security in the context of using the "Internet of things" in medicine // Medical Law. 2019. N 1. pp. 31-37; Blinov S.V., Kuzmina N.M., Revina S.N., Sidorova A.V. Basic approaches to defining the content of the term "telemedicine" // Lawyer. 2019.N 5. pp. 58-63., Etc.

[7] Carlisle G., Whitehouse D., Duquenoy P. (Eds.). eHealth: Legal, Ethical and Governance Challenges. Springer. 2013. 385 p.; Adams S., Purtova N., Leenes R. (Eds.). Under Observation: The Interplay Between eHealth and Surveillance. Springer, 2017. 210 p.; Gilroy A., Spontoni C., Llewellyn K., Undine von Diemar. Data protection challenges for telemedicine in the EU and US // E-Health Law & Policy. 2015. Vol. 2. Issue 8. P. 12-14.; Lynn D. Fleisher, James C. Dechene. Telemedicine and E-Health Law. Law Journal Press. 2014. 1080 p.; Callens S. E-Health & the Law. Kluwer Law International. 2003. 183 p.; E-health, privacy, and security law: 2014 cumulative supplement / Editor-in-chief W. A. H. Gantt III. – 2nd ed. – Arlington: The American Bar Association: Bloomberg BNA, 2015. 538 p.; Mantovani E., Quinn P. mHealth and data protection – the letter and the spirit of consent legal requirements// International Review of Law, Computers &Technology. Volume 28, 2014. Issue 2. P. 222-236; etc.

The study of the legal aspects of information security in telemedicine is also based on the works of foreign scientists - specialists in the field of information technology law. General theoretical developments in the field of information technology law, which served as the basis for this study, are set out in the works of scientists from the United States (USA) - L. Lessig, V. Cerf, the United Kingdom (UK) - I. Lloyd, A. Murray, D. Bainbridge, European Union countries - L. Bygrave, K. Mathiesen, D. Schartum, K. Demetrius, S. Magnusson. Particular legal issues of telemedicine and ehealth, including issues of electronic document management and personal data protection, are elaborated in the works of scientists from the USA, UK, Belgium, the Netherlands, Italy, Germany, India - J. Dumortier, G. Karlis G. Carlisle, D. Whitehouse, N. Purtova, S. Adams, R. Leenes, A. Gilroy, S. Callens, C. Spontani, E. Kosta, B. Koops, A. Wernick, I. Klünker, D. Gant, E. Mantovani, P. Quinn, L. Fleisher, J. Dechene, R. Sony, D. Sao, A. Gupta, and others.

The object and particular subject matter of the research

The object of the research is public relations in the field of using information technologies in medicine and protecting data processed in health information systems. The particular subject matter of the research is the regulatory framework of information security in telemedicine, legal tools of protecting electronic document exchange in telemedicine, the legal regime of data processed in health information systems.

The purpose and tasks of the research

The purpose of the study is to identify trends in the legal support of information security in telemedicine, to develop scientifically reasoned proposals for the development of legal tools of protecting electronic document exchange in telemedicine and the legal regime of data processed in health information systems.

Research tasks:

determine the correlation between the right to medical care and the right to access information in the information society;

to determine the role of legal support of information security for the development of telemedicine;

identify legal approaches to the regulation of health information systems and electronic health records that ensure the balance of public interests, rights and legitimate interests of patients;

to determine the legal tools of ensuring electronic document exchange in telemedicine that facilitate interoperability, protection of rights and legitimate interests in telemedicine;

to establish the peculiarities of processing health personal data in the new technological context and justify changes in the legal regime of personal data, taking into account the needs of telemedicine;

to identify the criteria for differentiating the legal regimes of health personal data and medical secrecy.

The research methodology

The methodological basis of the research includes general scientific methods: systemic, dialectical, analysis and synthesis, induction and deduction. Comparative legal method used in comparison of legislation on telemedicine in the Russian Federation and foreign countries. All the above mentioned methods, theoretical modeling, classification made it possible to solve the problems posed in the study and develop theoretical provisions of information law about the features, patterns and directions of legal support for information security in telemedicine, to offer practical recommendations for the development of legal regulation in telemedicine.

Empirical base of the research

The empirical base of the study includes the current regulatory legal acts of the Russian Federation and foreign countries, documents of international organizations, acts of courts, official statistics of Russian and foreign organizations, draft regulatory legal acts, etc.

The scientific novelty of the research

The scientific novelty of the work is that it is the first dissertation research of the legal aspects of information security in telemedicine in Russian legal science. The identified trends in the interaction of the right to health medical care with information rights, the developed approaches to the legal support of electronic

document exchange and the protection of personal data in telemedicine can serve as a theoretical basis for further research in the field of legal regulation of telemedicine and information law in general.

General conclusions of the research

1) In the information society, the right to medical care is closely interconnected with the right to access information. The right to access information guarantees the exercise of the right to medical care, determines its content and facilitates the achievement of equal access for every person to medical care.

2) Information security is a key condition for exercise of the rights and legitimate interests in telemedicine. In the legal support of telemedicine, information security plays a system-forming role and largely determines the direction for development of legislation on telemedicine both in the Russian Federation and in foreign countries.

3) One of the principles of information security is interoperability, which should be understood not only as a technical principle of interaction between information systems, but also in a broader (social) sense - as a principle of systemic informational interaction of subjects in the legal relations. On the example of the interaction in telemedicine, it is reasoned that interoperability is a new principle of information law that affects the development of legal relations in the context of digitalization.

4) Ensuring the balance of private and public interests in telemedicine requires differentiation of the grounds for processing health personal data. As an additional ground for processing personal data for certain purposes, it is proposed to presume the consent of the data subject to processing of data with the right to refuse from such processing (opt-out). These particular purposes may be, for example, the processing of electronic health records in the Unified state health information system, the processing of anonymized personal health data for research purposes. This approach, on the one hand, facilitates the protection of public interests in health care, on the other hand, it takes into account the autonomy of the data subject, his (her) privacy interests.

5) The exercise of the right to medical care, as a general rule, should not be conditioned by mandatory identification and authentication of the patient through a Unified state system of identification and authentication. Requirements for patient identification and authentication in telemedicine should be technologically neutral and applied with patient consent, unless identification and authentication are required in the legitimate interests of third parties. Legislation should guarantee the patient`s right to receive anonymous medical care using telemedicine technologies in cases that do not require mandatory identification of the patient and disclosure of his identity to third parties (including medical staff).

6) In order to eliminate collisions and duplication of requirements for data processing in telemedicine the legal regimes of personal data and medical secrecy have to be distinguished. To differentiate these legal regimes, it is proposed to recognize the priority of the legislation on medical secrecy over the legislation on personal data. Legislation on personal data has to be applied to the processing of medical data only in cases not covered by the regime of medical secrecy.

Theoretical and practical significance of the research

The theoretical significance of the research is the expansion of scientific ideas about the legal support of information security in the context of information society. The research results can be used in theoretical developments of the legal issues of information security not only in telemedicine, but also in other spheres undergoing digitalization.

The practical significance of the study is proposing recommendations for the development of legal regulation in the field of information security in telemedicine: a legal model for creating electronic health records and health information systems; legal tools for protecting electronic document exchange in telemedicine; requirements for the processing of personal data in telemedicine; guarantees of the right to anonymous medical care, differentiation of legal regimes of personal data and medical secrecy.

Reliability and approbation of the research results

The dissertation was carried out at the International Laboratory for

Information Technology and Intellectual Property Law of the National Research University Higher School of Economics. The provisions of the dissertation research are reflected in the articles[8] published in Russian and foreign academic journals, including those recommended by the Higher Attestation Commission of the Ministry of Education and Science of the Russian Federation, indexed in the Scopus and Web of Science databases, included in the HSE list of high-level journals.

The main provisions and conclusions of the research were presented at research seminars of the International Laboratory for Information Technology and Intellectual Property Law of the Higher School of Economics, at Russian and international scientific conferences[9] on information law issues, as well as in the reports published after these events.

Certain provisions of the study were used in the teaching activities of the author at the educational programs[10] of the Law Faculty of the National Research University Higher School of Economics, in research projects of the National Research University Higher School of Economics.

The structure of the research is predetermined by its subject, purpose and tasks and consists of an introduction (the general characteristic of the work); two chapters with six sections; conclusion and references.

---

[8] Zhuravlev M., Brazhnik T. Russian data retention requirements: Obligation to store the content of communications // Computer Law & Security Review. 2018. Vol. 34. No. 3. pp. 496-507; Zhuravlev M.S. Personal Data Protection in Telemedicine // Pravo. Zhurnal Vysshey shkoly ekonomiki. 2016. No 3. pp. 85-94; Zhuravlev M.S. Interoperability as a Factor of Law Development in the Digital Economy (eHealth case) // Pravo. Zhurnal Vysshey shkoly ekonomiki. 2019. No 3. pp. 98-116; Zhuravlev M.S. E-Health: Establishment and Development // Pravo. Zhurnal Vysshey shkoly ekonomiki. 2016. No 2. pp. 235-241; Zhuravlev M., Blagoveshchenskaya O. Telemedicine: Current State and COVID-19 Lessons // Legal Issues in the Digital Age. 2020. No. 2. pp. 92-143; Zhuravlev M.S. Legal Support of Electronic Document Management in Telemedicine // Informational Law. 2017. No 4. pp. 10-15.

[9] Zhuravlev M. eHealth regulatory challenges in Russia, in: The futures of eHealth. Social, ethical and legal challenges. Berlin: Alexander von Humboldt Institute for Internet and Society, 2019. pp. 143-150; Zhuravlev M.S. Personal Data Protection in Telemedicine // In. Law and information: the questions of theory and practice: a collection of materials of the international scientific and practical conference. Vol 6. Saint-Petersburg.: Presidential Library. 2017. pp. 151-154.

[10] As part of the course "Information technology in the activities of a lawyer" (2017-2018, 2018-2019), "Information law" (2018-2019), research seminars "Law and the Internet" (2016-2017) and “Law in the Digital Environment” (2017-2018, 2018-2019, 2019-2020).

BRIEF SUMMARY OF THE RESEARCH

The **Introduction** substantiates the relevance of the research topic, reflects the degree of its elaboration in legal doctrine, defines the goals and objectives of the work, the research methodology, indicates the main results of the research, confirms the degree of reliability and approbation of the results.

Chapter 1 "Legal challenges in the development of telemedicine" devoted to the analysis of general trends in the development of the right to health protection and medical care in a post-industrial (information) society, identifying tendencies in the development of legal relations in telemedicine, defining the role of information security in the legal background of telemedicine.

Section 1.1. "The right to health care and medical care in the information society" contains an analysis of the international and national legal foundations of the right to health care and medical care, reveals the peculiarities of ensuring and implementing this right in the post-industrial era.

Provision of medical care via telemedicine technologies is not a new human right, but it is a way of more efficient exercising the right to health care and medical care in the context of ICT development. In the information society, a person gets more guarantees that ensure equality in access to high quality medical care. The main drivers for these guarantees are distant interaction, personalization and automation.

In addition to ensuring equal access to medical care, information technologies provide more possibilities for patients to choose a doctor and a medical organization without being tied to specific territory, ensure continuity in the provision of medical care when a patient's or doctor`s place of residence changes. Telemedicine technologies provide the patient with constant access to information about his health status through electronic medical records. The patient's right to health prevention can be ensured through dynamic monitoring of health status with Internet of things technologies (apps and devices). The right to the provision of emergency medical care is more effectively realized through the use of telemedicine devices, which

make it possible to transmit information quickly to medical organizations in the need for urgent medical care and provide emergency medical care in a remote form. Artificial intelligence and machine learning that analyze medical data change approaches to diagnosis of patients, increases the efficiency and accuracy of decision-making in medicine.

The right to medical care via telemedicine technologies is directly related to the right to access information (including access to ICT) and depends on eliminating the digital divide. The social state of the post-industrial era in the modern technological context is obliged to create legal and infrastructural conditions for exercising the socio-economic rights of citizens using the potential of ICT (including the right to medical care via telemedicine technologies)

Section 1.2. "Development of the legislation on telemedicine" contains a comparative legal analysis of approaches to the regulation of telemedicine, outlines specifics of legal relations in telemedicine, reveals legal barriers to telemedicine and possible ways to overcome them.

Telemedicine is an interdisciplinary concept at the intersection of different areas: medicine, information technology, management, etc. With the development of legislation on different aspects of telemedicine, this concept is legally defined in various legal systems.

Based on the comparative legal analysis and the objectives of this study, the term “telemedicine” is proposed to be understood in the meaning of the use of ICT for provision of medical services, creation and maintenance of health care infrastructure, improving the quality and accessibility of health care. In this sense, telemedicine includes health information systems, electronic health records of patients, remote medical services, remote monitoring of the health status, issuance of electronic documents (prescriptions, sick leaves, medical reports and certificates), electronic appointment to a doctor, remote consultations of doctors and other forms of medical activity, including medical research, in which information and communication technologies are involved. The key characteristics of telemedicine are the remote interaction automated data processing.

The concept of telemedicine is dynamic. It incorporates new technological advances over time, responds to health care challenges, adjusts to the social and economic context.

Legal support of telemedicine is associated with a wide range of sectoral issues. Since traditional legal mechanisms do not take into account the peculiarities of telemedicine, there is a need to adopt new legislation aimed at protecting the rights and legitimate interests of patients and telemedicine actors and eliminating unreasonable legal barriers that impede the use of telemedicine technologies.

Barriers to the implementation of telemedicine can be organizational and technical (underdeveloped network infrastructure, peculiarities of information processing technologies, etc.), ethical (low level of digital literacy, mistrust to technologies, etc.) and legal (requirements to licensing of medical activities, restrictions on the processing of personal data, etc.). Legal barriers can be reasonable (legitimate) and unreasonable (illegitimate). Legitimate legal barriers are designed to ensure a balance of rights and legitimate interests. Unreasonable (illegitimate) legal barriers include outdated legal norms and institutions or gaps in the law. These barriers hinder the development of information technologies and need to be eliminated.

Telemedicine is a field that requires a special governmental strategy aimed to ensure high safety standards, protect the rights of patients. Many countries are adopting strategies and developing legal acts in order to remove legal barriers to the introduction of digital technologies in medicine and healthcare. All the studied jurisdictions (the USA, EU countries, Russian Federation) formed generally uniform approach to the regulation of telemedicine. Nevertheless, all these jurisdictions have their particular characteristics predetermined by legal traditions, socio-economic, cultural, and demographic factors.

For example, in the United States, states have broad competence in the field of health care. The issues of mutual recognition of licenses, conflicts of law issues and other aspects of cross-border provision of telemedicine services come to the fore on the agenda of legal regulation in the USA. Similar problems are relevant for

supranational regulation in the EU. The Russian approach to the legal regulation of telemedicine similar to the approach implemented in the EU countries at the national level. Special attention in Russian legislation is paid to data protection aspects and electronic document management in telemedicine.

The main legal barriers to the development of telemedicine, along with ensuring information security, include requirements for the diagnosis and treatment of patients, issues of licensing medical activities and cross-border provision of telemedicine services, issues related to legal liability and health insurance.

In most of countries, there is a tendency to move from strict prohibitions on remote diagnosis and prescribing treatment to flexible restrictions based on the specificity of the disease and the possibilities of remote interaction. The research reasons the necessity to follow the same approach to remote diagnosis and treatment in the Russian Federation.

Requirements for licensing telemedicine activities should take into account the specifics telemedicine technologies. In particular, there is no need in to require from an applicant the availability of premises (structures, buildings). It is advisable to provide additional requirements in terms of ensuring information security of software and information systems used to provide telemedicine services. In addition, the professional level of medical staff must be confirmed by documents on advanced training in the use of telemedicine technologies.

Legal relations in telemedicine are characterized by a wide range of subjects, which includes both primary participants (patients, physicians, hospitals) and secondary subjects that facilitate provision of telemedicine activities (operators of telemedicine platforms, ISPs and other entities which provide infrastructure). Changes in the range of subjects and transformation of their role in provision of telemedicine services entail changes in approaches to the regulation of medical activities, differentiation of requirements for “classical” and telemedicine actors.

Active development of Internet services (aggregators) in telemedicine raises the issue of adopting special regulation of the activities of telemedicine digital platforms. The owners of these platforms do not only provide infrastructure for

provision of telemedicine services, but actually carry out operational activities in provision of telemedicine services (in this sense digital platform is gradually "replacing" the medical organization). Such changes entail a number of subsidiary problems related to licensing, distribution of legal responsibility between doctors and platforms, consumers rights protection, etc.

Section 1.3. "Information security in telemedicine: specifics of legal relations" outlines the legal issues of information security in telemedicine and their role in the legal regulation of telemedicine.

Ignoring the problems of information security eliminates all the advantages of telemedicine technologies. Confidence of patients in new technologies, their readiness to transfer an extremely important sphere of their private life into the "hands" of computers, communication networks, information systems and algorithms depends on the degree of information security. Ultimately, the physical safety of patients depends on information security in telemedicine.

Other legal aspects of telemedicine are in one or another way related to information security issues and indirectly perform the function of ensuring information security. Thus, licensing requirements for telemedicine should cover the requirements for information security of medical devices and software, guarantee the expertise of medical staff in handling telemedicine technologies. Establishment of due contact with the patient and access to his medical history is carried out through identification and authorization procedures. Liability issues include liability for improper operation of information systems, illegal processing of personal data, disclosure of medical secrets and other offenses in the information sphere that may entail negative consequences for patients. Insurance can cover cybersecurity risks in telemedicine, etc.

The interdisciplinary nature of the abovementioned issues characterizes information security not as a local or secondary problem, but as a general, universal and integral part of the transition from traditional healthcare to telemedicine and e-health. The developed approaches to ensuring information security in telemedicine can be considered as a model for solving similar problems of digitalization in other

spheres of public life.

The broad approach to information security adopted in the Russian legal doctrine comprehensively covers all issues related to information legal relations, both protective and regulatory. Such a broad definition of information security is useful in the context of building governmental policy in the information sphere. However, this approach does not allow to highlight a specific subject of legal regulation.

In order to study the legal aspects of information security, it is necessary differentiate the information security issues in telemedicine. Methodologically, the legal aspects of information security are proposed to be divided into two groups. The first are designed to provide information exchange (data sharing) in telemedicine. The second group of issues concerns countering cyber threats.

The legal aspects of data sharing, which are the main subject of this study, include the legal regime of data used in telemedicine and the legal support of electronic document exchange in telemedicine. The legal regime of data establishes the legal properties of data (who owns data, by whom and for what purposes it can be used, etc.). Electronic document exchange issues include legal framework for creating electronic health records, organizing health information systems, their interaction and requirements for processing information in these systems.

The legal aspects of cybersecurity (countering cyber threats) in telemedicine include protection of critical information infrastructure in the health sector, requirements for the personal data protection in health information systems, as well as liability issues concerning offenses in the use of health information systems. The basis for countering cyber threats are technical requirements for the security of information systems and legal liability for violation of security requirements. It seems that these issues do not have such specificity in the field of e-health that significantly distinguish it from other fields, therefore they are not the main focus of this study.

In the information society, there is a more active involvement of privacy sphere in public spheres (in the spheres of public governance, statistical and

scientific research, etc.). Changing technological and social context (especially during the COVID-19 pandemic) raises questions on finding a new balance between public interests, the right to access information and the right to privacy in the field of health. A new approach to the regulation should be based on a “win-win” strategy “with non-zero-sum”, without derogation of privacy rights. Such a regulatory strategy can be implemented if restrictions on the right to privacy are offset by information security measures to effectively protect the interests of individuals.

Chapter 2 "Legal regulation of information security in telemedicine" reveals the legal aspects of electronic document exchange in telemedicine and proposes the directions for adaptation of the Russian personal data legislation to the needs of telemedicine.

Section 2.1. "Legal aspects of electronic document exchange in telemedicine" focuses on the legal models for creating electronic health records, organizing health information systems and secured interaction between telemedicine actors.

For the functioning of electronic document exchange in telemedicine, electronic health records of patients (EHR) are created. EHR are integrated into health information systems (HIS). The chosen approach to the creation of EHR and HIS directly influence on the possibilities of data sharing and interaction between telemedicine actors.

In different countries, two legal mechanisms for creating electronic health records have become widespread - “opt-in” and “opt-out”. The “opt-in” mechanism is largely based on the autonomy of patients' will, a conscious choice to participate in the electronic exchange of medical information. The use of such a mechanism entails a greater degree of responsibility of the patients for their choices, including the choice of the person to whom they have entrusted the storage and management of their personal electronic health records. Despite the obvious positive characteristics of this mechanism, it has a significant drawback - it complicates creation of a unified information space in telemedicine, leaves the medical data of a large number of patients outside the electronic document flow. The “opt-out”

mechanism allows creating electronic records of patients' health without their consent but with possibility to refuse and exclude them from electronic document exchange. Such a mechanism involves the largest possible amount of medical information in the electronic document flow, but at the same time respects the will of patients.

There are no specific rules for creating electronic health records in the Russian Federation. In order to eliminate uncertainty in legal regulation, it seems necessary to enact the “opt out” mechanism for creating electronic health records: to establish the obligation of a medical organization to inform patients about creation of electronic health records, to preserve the patient's right to refuse from electronic health records and provide the procedure for exercising this right, explaining the consequences of refusing electronic records.

In different jurisdictions, three general models of health information systems (HIS) have been implemented. These models differ in the ways of storing and managing medical information: decentralized, centralized and patient-oriented. The centralized model is most convenient for operation and interaction, but it has higher degree of vulnerability in terms of personal data protection (concentration of all patient data in one place increases potential harm from cybersecurity incidents). Other models, at first glance, are more consistent with ensuring information security (due to distributed storage of information and taking into account the patient's choice, etc.), but at the same time they create more obstacles for data exchange. In addition, decentralized storage does not guarantee absolute security, and a breach of security even on one of the elements of a distributed system can also cause significant damage to patients and other entities.

In Russia, a centralized model of HIS is being formed. However, it does not imply the storage of all health data on a single server. The unified state healthcare information system (“EGISZ”) plays the role of infrastructure platform and coordinator of data exchange. The centralized management of health information systems allows rapid data exchange both within the system and with external users /data providers. This approach seems to be optimal, since it consolidates to the

unified system only part of patients` data that is necessary for general operational purposes.

The set of tools for ensuring information security of electronic document exchange in telemedicine includes procedures of identification and authentication; differentiation of access rights to health records; anonymization and pseudonymization of data, requirements for the safety of medical devices, etc.

The current Russian legislation provides the possibility of using only a unified identification and authentication system (ESIA) and qualified electronic signature in telemedicine. For the development of telemedicine market, especially in the private sector, a more flexible approach to the identification is required. Identification and authentication methods need to be complied with technologically neutral requirements, should be reliable and provide the integration of patient data into the Unified State Health Information System ("EGISZ").

In order to guarantee the patients' right to anonymous medical care, the research proposed two mechanisms for the provision of anonymous medical care with telemedicine technologies: 1) pseudonymization of telemedicine consultation for a medical professional, which implies preliminary identification of the patient in the information system and subsequent depersonalization of the patient's medical profile for medical staff (while the patient's anonymity is provided only in the context of interaction with a doctor, however, the information is fully integrated into the Unified State Health Information System); 2) pseudonymization of telemedicine consultation without transferring data to EHR and integrating it with the Unified State Health Information System.

The right to anonymous medical care with telemedicine technologies should be granted in all cases, if it does not affect the quality of medical care and it is not limited by legal requirements. Telemedicine platforms, devices and information systems should provide for technical possibility of pseudonymization of telemedicine consultation. It is reasonable to stipulate such functional features in the relevant technical requirements.

In order to implement the patient's right to access EHR, as well as to ensure

transparency of access to these records, it is necessary to set the technical ability for patient to control all the access cases to EHR through getting consent and logging of all requests for access to his EHR.

The paper supports the idea of differentiating medical devices and applications used in telemedicine into specialized (professional) use and general (wellbeing) use. Accordingly, the requirements for device manufacturers and developers of telemedicine applications also have to be differentiated. Wellbeing devices and software should not be classified as medical devices and the state registration procedure should not apply to them. However, some requirements for these devices and software still need to be stipulated. Thus, manufacturers and sellers should inform the consumer about the purpose of using the device / application, restrictions on its use, possible errors in measuring physiological parameters, etc.

To improve the information security of medical devices, it is necessary to maintain the principles of built-in security (embedded security) and privacy by design. These principles should be taken into account in developing standards, technical regulations, preparing technical specifications etc.

Section 2.2. "Personal data protection in telemedicine" analyses the legal regime of health personal data, provides proposals for adapting the legal regime of personal data to the needs of telemedicine and eliminating conflicts between personal data legislation and provisions on medical secrecy.

The legal issues of adapting the legal regime of personal data to the needs of telemedicine (and digital economy in general) include: changing approaches to the consent to processing personal data; expanding the grounds for processing personal data for publicly significant purposes (including statistical, research purposes); improving the legal regime of anonymized personal data; strengthening the role of the data subject in the management and protection of his personal data.

The conceptual drawback of existing binary model for processing personal data (with consent - without consent) is the complete disregard of the will of the data subject in cases established by law. One of systemic changes in the legal regime of personal data is the differentiation of approaches to consent depending on the public

interest. If there is a public interest in the processing of personal data, it is possible to use two models of regulation: 1) allow personal data processing regardless of the consent (without consent); 2) allow personal data processing without the consent until the data subject expresses disagreement with the processing of personal data (the so-called “opt-out” model). Both models could be used to implement public interests and differentiate depending on specific goals and needs, taking into account a reasonable and sufficient restriction of the data subjects` will.

The opt-out consent model for the processing of personal data can be widely used in telemedicine. For example, such a model founds the legal basis for the default (opt-out) implementation of EHRs. Also, this model can be used to organize a search system for participants in medical research (including clinical trials of drugs), if the research requires a sample of patients of a certain category (with a specific disease, with specific physiological characteristics, etc.). On the one hand, such a model will create an effective mechanism for attracting citizens to participate in research. On the other hand, it will provide patients with the opportunity to refuse to participate in this system.

In addition to the “opt-out” model, a model of framework (general) consent to the processing of personal data is proposed, which is a private form of the “opt-out” model, in which the “opt-out” consent mode is not established by the legislator in relation to any operator and any subject of personal data, but privately between a specific operator and a specific data subject. A data subject can give to a specific operator a framework consent to the processing of personal data for purposes that will be determined by the operator in the future. The operator, in turn, undertakes to notify the subject of personal data about the new purposes and methods of processing personal data. The operator is obliged to provide the data subjects with adequate organizational and technical means (for example, by using the platform for managing consent to the personal data processing) to be informed with the goals of processing and refuse from undesired forms of processing.

The particular attention is paid to the issues of health personal data protection for research purposes, as well as to the issues of data anonymization and

depersonalization. The paper proposes several recommendations on the development of the relevant legislation.

First, the possibility of processing depersonalized data for research and statistics purposes without the consent of the data subject should be also extended to special categories of personal data, including health data.

Secondly, it is recommended to provide centralized procedure for providing depersonalized health data from the Unified State Health Information System ("EGISZ") for research and statistical purposes. At the same time, transparency, non-discrimination in access to such data should be ensured, as well as ethical control over the use of health personal data.

Thirdly, it is necessary to distinguish between reversibly depersonalized (pseudonymized) data and irreversibly depersonalized (anonymized) data. The definition of reversibly depersonalized (pseudonymized) data can be left within the framework of the existing definition of depersonalized data (personal data that cannot be correlated with a specific person without using additional information stored separately and in relation to which sufficient measures have been taken to protect it from being correlated with depersonalized personal data). Irreversibly depersonalized (anonymized) data is data that cannot be correlated by reasonable means with a directly or indirectly identified or identifiable natural person. In terms of its legal consequences, irreversible depersonalization should be equated to destruction of personal data and be excluded from the requirements of personal data legislation.

It is important to keep in mind the dynamic and contextual nature of the reasonable means for identifying the data subject. The paper proposed to develop mandatory minimum criteria for depersonalized data and a basic methodology for their depersonalization (both reversible and irreversible), without which the data cannot be recognized as such. Each operator intending to process depersonalized data must use its own criteria and methodology for anonymization (not lower than the mandatory minimum requirements), taking into account the specific risks of correlating this data with an individual. At the same time, the operator must bear

risks in the form of legal liability for insufficient depersonalization. Such legal risks will be reasonable price for the possibility of more free use of depersonalized data, and the operator will be interested in taking more reliable measures to protect data from reidentification.

In the current Russian legislation, there are conflicts between the legislation on personal data and the provisions on professional secrets, including medical secrets, which create unreasonable barriers for processing health data.

In the context of implementing IT in medicine there is a convergence of spheres traditionally regulated by personal data protection law and legislation on medical secrecy (transmission, storage and other processing of medical information is carried out with using automation tools). This process intensifies the contradictions between the rules on the protection of personal data and medical secrecy, which necessitates the differentiation of their subjects of regulation. As a direction of such a distinction, it is proposed to establish the priority of special legislation on medical secrecy and the subsidiary application of legislation on personal data to the processing of health data in cases that go beyond the regulation of medical secrecy.

Section 2.3. "Interoperability as a principle of information security in telemedicine" considers interoperability as a system-forming principle of interaction between health information systems and telemedicine entities.

In the digital society interoperability should be understood not only as a technical principle of interaction between information systems, but also in a broader (social) meaning - as a principle of systemic interaction of subjects. In this meaning, interoperability should be considered as a new principle of information law and as a factor of legislation development in the context of digitalization. Interoperability is a condition for the transition of e-government to a new stage of development, in which public services are not only transferred to electronic format, but also receive qualitatively new (digital) content through prompt information exchange, remote interaction and modern data processing technologies.

In order to create an interoperable "ecosystem", the interaction of information

systems and subjects of telemedicine activity should be built on the basis of the following principles that ensure the classic triad of information security - availability, integrity and confidentiality of information (confidentiality, integrity, accessibility - CIA): integration and expansion of communication channels of information systems (integration); expanding the area of use of information systems (reusability); ensuring the mobility and dynamism of data processed in information systems (dynamism); ensuring the right of patients to access and manage personal electronic records (patient empowerment).

The lack of a unified technical, organizational and legal basis for data processing in health information systems is a significant barrier to information exchange and development of telemedicine. In order to eliminate this barrier and achieve a synergistic effect from information interaction, it is necessary to use uniform standards for collecting, storing, processing and exchanging data, which will ensure the interoperability of information systems.

The paper proposes directions for the development of interoperability in the field of e-health, including standardization, transparency and openness, multipurpose use of data, technological neutrality and other directions, each of which is outlined in the context of legal issues that must be taken into account in the process of their implementation.

The legal framework for interoperability mainly covers the interaction of public information systems. However, in the context of building a digital economy, interoperability is necessary not only in the public sector, but also between private entities. Interoperability in the private sector is gaining relevance in connection with the recognition of the right to data portability and its legislative framing (in particular, in EU legislation). In telemedicine, the right to data portability can be realized by "transferring" patient's EHR in one medical organization to a patient's EHR in another medical organization, thereby ensuring the integrity and continuity of data (for example, in order to monitor the long-term dynamics of health parameters, results of medical tests, etc.).

In the **Conclusion**, the general ideas of the study are summarized and

perspective directions for further research of the topic are considered.

The main conclusions of the research are reflected in the following publications:

1) Zhuravlev M.S. Interoperability as a Factor of Law Development in the Digital Economy (eHealth case) // Pravo. Zhurnal Vysshey shkoly ekonomiki. 2019. No 3. pp. 98-116.
2) Zhuravlev M., Brazhnik T. Russian data retention requirements: Obligation to store the content of communications // Computer Law & Security Review. 2018. Vol. 34. No. 3. pp. 496-507.
3) Zhuravlev M.S. Personal Data Protection in Telemedicine // Pravo. Zhurnal Vysshey shkoly ekonomiki. 2016. No 3. pp. 85-94.
4) Zhuravlev M.S. E-Health: Establishment and Development // Pravo. Zhurnal Vysshey shkoly ekonomiki. 2016. No 2. pp. 235-241.
5) Zhuravlev M., Blagoveshchenskaya O. Telemedicine: Current State and COVID-19 Lessons // Legal Issues in the Digital Age. 2020. No. 2. pp. 92-143.
6) Zhuravlev M. eHealth regulatory challenges in Russia, in: The futures of eHealth. Social, ethical and legal challenges. Berlin: Alexander von Humboldt Institute for Internet and Society, 2019. pp. 143-150
7) Zhuravlev M.S. Legal Support of Electronic Document Management in Telemedicine // Informational Law. 2017. No 4. pp. 10-15.
8) Zhuravlev M.S. Personal Data Protection in Telemedicine // In. Law and information: the questions of theory and practice: a collection of materials of the international scientific and practical conference. Vol 6. Saint-Petersburg.: Presidential Library. 2017. pp. 151-154.