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

CONTEMPORARY LEGAL ISSUES ON NEW TECHNOLOGIES

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

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

СОВРЕМЕННЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ НОВЫХ ТЕХНОЛОГИЙ

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

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

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

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

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

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

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

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

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

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

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

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

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

Cybersecurity in International Law

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

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

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

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

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

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

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

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

Digital intelligence in the diplomatic corps

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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