IRSTI 10.87.27

Zh.T. Iskakova
T.S. Kadyrzhanova

L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
(E-mail: ziskakova@list.ru, qadyrzhanova@gmail.com)

Analysis of problems and challenges in the legislation of the Republic of Kazakhstan on personal data protection and international legal regulation

Abstract. *The authors analyze the international legal and national legal regulation in order to study, determine the level of regulatory security of identification and authentication of individuals and legal entities for the purpose of their legally significant actions in various areas of public relations in the Republic of Kazakhstan.*

The authors have attempted to formulate certain conclusions and proposals. On the one hand, these formulated recommendations will enable the state to ensure the level of trust of citizens and legal entities in the field of electronic information interaction. On the other hand, the same proposals will reduce the risks associated with leaks of biometric databases of users of information systems, and contribute to maintaining the confidentiality of biometric personal data of individuals and legal entities. As well as the recommendations aim at improving efficiency in the field of public-legal and private-legal relationships carried out through electronic services.

Keywords: *biometrics, biometric data, personal data, biometric identification, digital identification, authentication, GDPR.*

DOI: https://doi.org/10.32523/2616-6844-2022-141-4-48-60

Introduction

The rapid development of artificial intelligence, with biometric technologies represented by "face recognition", "fingerprint verification", "voice unlocking" and "iris recognition" have flourished and are widely used in criminal investigation, public safety, finance, healthcare, transportation, schools, payments, communities, businesses, and other scenarios. It plays a vital role in the development of network technologies, big data and even the digital economy and has become an important part of the national economy. This kind of information obtained by special technical processing of physical, physiological, or behavioral characteristics of individuals using biometric technology is "personal biometric information», such as fingerprints, iris, facial features, voice, gait, handwriting, etc. Since personal biometric information is unique and unchangeable, it will never be recovered after it is leaked, which can lead to risks such as invasion of privacy, violations of laws and crimes, racial discrimination, and a threat to national security. Vigilance is urgently needed.[1]

For example, Facebook, which has recently been widely discussed, has triggered a class action

[1] Kukharev G. A. Biometricheskie sistemy: Metody i sredstva identifikatsii lichnosti cheloveka [Biometric systems: Methods and means of identification of a person], Politekhnika. pp. 240. (2001). [in Russian]

lawsuit for compensation of $5,550 million due to facial recognition technology. A citizen sued the company for the forced collection of information about individuals, 170,000 data about individuals were publicly sold.[2] Thus, in the face of challenges related to biometric technologies, the question of how to protect personal biometric information has become a key issue of global concern. Among the various mechanisms for the protection of personal biometric information, providing a basis for the use and protection of personal biometric information through legislation is a prerequisite and key to regulating the abuse of personal biometric information and implementing the protection of personal biometric information. From the point of view of legal principles, general rules can reduce the costs of searching and learning information, which helps individuals to recognize the law as soon as possible and use it to protect their rights, and data collectors and processors performed compliance operations as soon as possible, and this also contributes to law enforcement agencies implementing enforcement as soon as possible.[3] Currently, many countries and regions have begun to develop appropriate legislation, but Kazakhstan has not yet formed a systematic legislative framework for protection, which leads to serious gaps in the protection of personal biometric information.

Materials and methods

The analysis of theoretical materials of research papers, publications allowed the authors to identify the fact that in legal science is not always clearly and reasonably formulated common approaches, but also provisions on legal problems and consequences of the introduction of biometric technologies in all spheres of human life.

To achieve the stated goals, the authors applied the method of system analysis, the research of leading legal scientists, as well as research from related sciences and scientific directions, such as biometrics and information technologies were used as materials.

Discussion

The legislative status of the protection of personal biometric information in Kazakhstan has relatively few norms on the protection of personal biometric information, mainly contained in the "Law on Identity Cards", "Law on Combating Terrorism", "Law on Network Security", "Law on the Administration of exit and Entry", "Criminal Law", "Criminal-Procedural law", "Civil Code", "Law on Protection of Consumer Rights and Interests" and other laws, "Regulations on Administration of Entry of Foreigners", "Regulations on administration of security Services", "Regulations on the Administration of Credit reporting" and other administrative regulations, as well as some less effective regulations and regulatory documents. This mainly concerns the principles of protection of personal biometric information, rules of use, regulatory bodies and functions, legal liability, remedies, etc.[4]

Firstly, the relevant provisions on the collection, management and protection of "fingerprint information" by public security agencies in such activities as case investigation, crime prevention and public security management.In accordance with the "Law on the Identity Card of a Resident", "Law on Combating Terrorism", "Criminal Procedure Law", "Rules for the Administration of Entry of Foreigners", "Rules for Conducting Administrative Cases Considered by Public Security Agencies" and other legal provisions, public security agencies can use personal biometric information, such as fingerprints, is used in the registration of identity cards, the management of entry and exit, the consideration of administrative and criminal cases, and we

[2] Afanas'ev A. A. Autentifikatsiya. Teoriya i praktika obespecheniya bezopasnogo dostupa k informatsionnym resursam [Authentication. Theory and practice of providing secure access to information resources], Uchebnoe posobie dlya vuzov: Grif UMO MO RF, Goryachaya liniya, Telekom, pp. 254. (2012). [in Russian]

[3] Barry, A. Ireland 'should consider laws that would jail cyber bullies' (TheJournal.ie. 2013). [Electronic resource] – Available at: https://www.thejournal.ie/cyber-bullying-ireland-1162881-Nov2013/ (Accessed: 03.09.2022).

[4] Gomez-Barrero M., Drozdowski P. Biometrics: Challenges and Opportunities // IEEE Transactions on Technology and Society. – 2022. [Электронный ресурс] - URL: https://arxiv.org/pdf/2102.09258 (дата обращения: 04.09.2022).

are obliged to maintain its confidentiality. In the event of a leak, it will be subject to administrative sanctions and will be investigated for criminal prosecution.

The second is to protect personal biometric information by clarifying the rights, obligations and legal responsibilities of the subjects of information of each party. For example, in the civil sphere, the Civil Code establishes the basic code of conduct for the protection of personal information and the main responsibilities of information processors to ensure information security. The collection of personal Rights in the Civil Code focuses on the protection of "private life" and contains detailed provisions on the principles of processing personal information, the rights of personal data subjects, as well as obligations to ensure the security and confidentiality of information processors. At the same time, the "Law on the Protection of Consumer Rights and Interests" establishes rules for the collection and use by operators of personal information of consumers and the obligations of operators to protect. In the criminal sphere, personal biometric information is indirectly protected by establishing criminal liability for violation of personal data of citizens. More typical is the provision of the Criminal Law on a crime related to the violation of personal data of citizens.

The third is to establish rules for various aspects of the collection, processing and use of personal biometric information. Relatively focused on the field of information management. For example, the "Law on Network Security" establishes rules for network operators on the collection and use of personal information. Network operators, network controllers and other organizations and individuals should not illegally obtain, sell, or provide personal information to others. Among them, "personal information" includes "personal biometric information". At the same time, Kazakh legislation has also realized that "personal biometric information" is different from general personal information and has introduced special provisions on personal biometric information. For example, the "Guide to the Protection of Personal Information on the Internet" contains special provisions on the "collection" and "public disclosure" of personal biometric information in the "Management Mechanism, technical security measures and business processes to ensure the security and protection of personal information". It should be noted that the "Personal Information Security Specification for Information Security Technology", revised on March 6, 2020, contains special provisions on the collection and storage of personal biometric information and clearly stipulates that «the collection of information about a person must be notified separately, and the original image should not be stored. In addition, they are also provided for by the rules of self-regulation of some industry associations. For example, the "Convention on Self-Regulation of the Autonomous Payments Industry for Face Recognition (Trial Implementation)" provides for autonomous payments for face recognition from the point of view of security management, terminal management, risk management, as well as protection of the rights and interests of users.[5]

Kazakhstan already has some provisions on the protection of personal biometric information, but the legislation is still relatively decentralized and cannot meet the needs for the protection of personal biometric information. Firstly, unique attributes are not highlighted, and there are no target provisions. The existing legislation does not single out the unique attributes of personal biometric information and mainly considers "personal biometric information" as a type of "personal information" subject to regulation, for example, the aforementioned provisions of the "Civil Code", "Law on Network Security" and "Law on Consumer Protection". Even if several legal norms recognize that personal biometric information is "confidential personal information", they just stipulate it in the links "collection" and "disclosure" and do not contain systematic targeted rules, such as "Personal data security Rules in the field of information security technologies".

Secondly, the legislative concept is unclear, and the expression is inaccurate. The concept of legislation is, in fact, a measurement of various

[5] Ben-Shahar O, Jacob L. S. Confidentiality Agreements: An Introduction [J], Journal of Legal Studies 2016 (2), pp. 51–61.

interests, guiding the path and value choice of legislation. Currently, there are doubts about the security and legality of the collection, processing, and use of personal biometric information at home and abroad, but various industries in Kazakhstan actively encourage the development and use of personal biometric information, and there is even a growing trend. Therefore, how to create a legislative concept and the measurement of interests between the protection and use of personal biometric information is the focus of legislation on the protection of personal biometric information. Currently, the legislative philosophy of Kazakhstan is unclear. For example, the "Law on Network Security" and the "Civil Code" regulate only "personal biometric information" as a type of "personal information", and the "Manual on the Protection of Personal information on the Internet" and "Specification of the security of personal information in information security technology" contain only special provisions on the collection, storage and public disclosure of personal information biometric information, none of which clearly indicates a legislative concept.

Thirdly, the legislation is fragmented, and the legal status is low. Currently, there is no uniform regulation of technical standards and mechanisms for the protection of personal biometric information, and systematic special legislation is needed. At the same time, the legal status of the norms for the protection of personal biometric information is small, and most of them are regulations, regulatory documents and even industry rules formulated by industry associations and enterprises. Although there are currently disputes over the right to privacy, new personal rights and ownership rights to personal biometric information, there is no doubt that they are all fundamental rights of citizens, so they should be regulated by legislation with a higher level of efficiency.

Fourth, the specific content is unclear, and systematic protection has not yet been formed. The current rules for the protection of personal biometric information are mainly based on fundamental and general provisions, and their efficiency is low. For example, the "Regulation on the Management of Security Services" provides only that public security agencies "must keep secrets", but there are no rules on how to keep secrets. At the same time, in terms of content, it focuses on establishing liability provisions and is scattered across various types of norms, such as the crime of violating citizens' personal information in the criminal sphere.; and there are no provisions on the legal attributes of personal biometric information, unique legal principles of protection, the relationship between rights and obligations, regulatory authorities and responsibilities, etc. As well as the above content are the basis for the protection of personal biometric information. Fifth, the object of protection is relatively narrow, and the applicable subject is relatively isolated. Due to the development of information technology, the current legislation pays more attention to the protection of "fingerprint information", and there are fewer provisions for the protection of other personal biometric information, such as information about the face, information about the iris, information about veins and information about the voice. Recently, with the rapid development and widespread use of "facial recognition technology", it has just begun to protect "facial recognition information". At the same time, most existing laws focus on regulating the collection of fingerprint information by public authorities, especially public security agencies, and there are relatively few provisions to protect the collection, processing, and use of personal biometric information by private organizations.[6]

The legislative model of personal biometric information refers to the legal form adopted by the State when adopting legislation on the protection of personal biometric information and related to the field of correction. The legislative model has a profound impact on the implementation of the protection of personal biometric information in terms of breadth, and this is the first problem that needs to be solved with the help of legislation on personal biometric information. The dual legislative model of personal biometric

[6] William Fry and Forbes. Europe for Big Data // Forbes Insights, 2016. [Электронный ресурс] - URL: http://www.williamfry.com/docs/defaultsource/reports/william-fry-europe-for-big-data-report.pdf?sfvrsn=0 (дата обращения: 05.09.2022).

information is based on differences in legislative tradition and prerequisites. The current legislative model for the protection of personal biometric information basically has two types: a special legislative model and a comprehensive legislative model. The model of special legislation refers to the model of protection of personal biometric information in the form of separate legislation. Some states in the United States are represented among them.[7] Much of the protection of personal biometric information in the United States is based on the protection of privacy. Since the 21st century, biometric technologies have been widely used in the fight against terrorism, national security, criminal investigations, and other areas and gradually began to be used for civilian purposes and commercialized in Illinois, Chicago, etc.

Currently, most states in the United States allow employers or companies to collect and analyze personal biometric information, but it is prohibited to profit from biometric information. Although the United States has not adopted uniform rules for the collection and use of personal biometric information at the federal level, each state has consistently formulated protection laws that specifically regulate the use of personal biometric information by the private sector. For example, Illinois passed the first "Biometric Information Privacy Law" in the United States in 2008. Texas adopted the "Law about the privacy of biometric information" in 2009, and Florida adopted the "Privacy Act of biological information" in 2019.[8]

In addition, Alaska, New Hampshire, and other states have gradually included biometric information laws on the legislative agenda. The applicable object of the aforementioned legislation is only the collection, processing, and use of personal biometric information by "private individuals". The content of the legislation mainly defines the legal concept, the relationship between powers and responsibilities, the code of conduct, regulatory bodies, and functions, as well as means and methods of facilitation. Since 2019, due to the widespread use of "facial recognition technology", the legality of the use of personal biometric information has again caused controversy. Bills have been introduced at both the state and federal levels specifically to protect "facial recognition information". In May 2019, the City of San Francisco, California, revised the "Stop Covert Surveillance" rules, arguing that facial recognition technology violates the privacy and freedom of citizens and can lead to racial inequality. It became the first city in the United States to ban official agencies from using facial recognition technology. In June 2019, the Somerville, Massachusetts City Council passed a "Comprehensive Ban on Facial Recognition Ordinance" that prohibits the use of facial recognition software by police and the public sector.[9] In July 2019, the City of Oakland, California, also promulgated the "Surveillance and Public Safety Act". At the federal level, the U.S. Senate passed the "Commercial Facial Recognition Privacy Act" in March 2019. On February 12, 2020, a member of Congress proposed in the Senate a draft "Law on the ethical use of Facial Recognition", the purpose of which is to suspend the use of facial recognition technology by government agencies. The Committee proposes appropriate guidelines and restrictions on the use of facial recognition technology. A comprehensive legislative model implies the absence of a distinction between personal biometric information and general personal information, the unified inclusion of

[7] Custers B., Van der Hof S., Schermer B., Appleby-Arnold S., and Brockdorff N. Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law // SCRIPTed, Journal of Law, 2013, Technology and Society, Volume 10, Issue 4, pp. 435–457. [Электронный ресурс] – URL: https://script-ed.org/article/informed-consent-social-media-gap-user-expectations-eu-personal-data-protection-law/ (дата обращения: 07.09.2022).

[8] Mason S. Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation // SCRIPTed, Journal of Law, 2012, Technology and Society, Volume 9, Issue 1, p. 327. [Электронный ресурс] – URL: https://script-ed.org/article/informal-debate-on-the-issues-relating-to-terminology-and-clarification-of-concept-in-respect-of-the-eu-e-signature-legislation/ (дата обращения: 06.09.2022).

[9] Отчет Secure Identity Alliance & the onepoint team "Giving Voice to Digital Identities Worldwide - Key insights and experiences to overcome shared challenges", 2021. [Электронный ресурс] – URL: https://secureidentityalliance.org/publications-docman/public/163-21-02-12-giving-voice-to-digital-identities-worldwide-en/file (дата обращения: 07.09.2022).

various types and types of personal information in the Law on the Protection of Personal Information and unified legislative protection from various aspects, such as administrative, civil, and criminal law.[10]

Currently, most countries and regions are adopting a comprehensive legislative model. The European Union is a typical representative of a comprehensive legislative model that has established a method of protection for strengthening administrative oversight of the public sector based on the rights of the individual.[11]

The "General Data Protection Regulation" (also known as the "GDPR"), which came into force in 2018. The GDPR provides for the protection of individuals in the processing of personal data and rules for the free flow of personal data. It provides for special protection of "biometric data" as "special types of personal data" and "in principle prohibits" the collection and processing of biometric data for the purpose of "identifying specific individuals" but provides for nine exceptions. At the same time, the GDPR allows Member States to set additional restrictions in their domestic legislation. It should be noted that the European Union is vigilant about the use of facial recognition technology.[12] In 2019, the EU Agency for the Protection of Fundamental Rights released "Facial Recognition Technology: Considerations on Fundamental Rights in Law Enforcement", which analyzes the problems that facial recognition technology poses for fundamental rights and briefly introduces the steps that public authorities should take to avoid human rights violations when they implement recognition technology individuals in real time to achieve the goals of law enforcement agencies. Asia has adopted legislation on the protection of personal biometric information relatively late and is heavily influenced by EU legislation. It also mainly uses a comprehensive legislative model. For example, in order to protect personal privacy related to personal data and clarify the flow and use of personal data, India promulgated Law No. 373 "Personal Data Protection Act" in 2019.[13]

Explaining the general rules for the protection of personal data, it provides special protection for "biometric data" as a special type of personal data and clearly stipulates that unless permitted by law, no authorized person should process biometric data notified by the central government. In general, both legislative models have their pros and cons. A specialized legislative model is focused and highly effective and can be flexibly formulated according to different areas, but conflicts may arise between different legislations; a comprehensive legislative model is more systematic, but flexibility is not enough. From the point of view of the content of legislation, regardless of which model is adopted, the legal principles, rules of protection, rights, and obligations to protect personal biometric information are generally consistent.[14]

The choice of a legislative model for the protection of personal biometric information should be based on an analysis of the causes, historical evolution and practical dilemmas of various legislative models in combination with legislative traditions, realistic needs, and the current situation of the development of the legal system in order to make a comprehensive judgment and strive for the best balance of interests between the protection of individual rights and interests and the development of groups. Judging by the traditions and trends in the development of information legislation in

[10] Vecchi D. and Marchese M. Italy: The Privacy, Data Protection and Cybersecurity Law Review // Law Business Research. – Chapter 15, 9th Edition, 2021. [Электронный ресурс] – URL: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review (дата обращения: 08.09.2022).

[11] .: List of acceptable supporting documents for verification. 01 июля 2022 года. [Электронный ресурс] - URL: https://uidai.gov.in/images/commdoc/valid_documents_list.pdf (дата обращения: 11.09.2022).

[12] Dar A., Viswanath N., Suri Sh. The Financial Technology Law Review: India // The Law Reviews – 5th Edition. – 2022. [Электронный ресурс] - URL: https://thelawreviews.co.uk/title/the-financial-technology-law-review/india (дата обращения: 11.10.2022).

[13] Yang H. The Privacy, Data Protection and Cybersecurity Law Review: China // The Privacy, Data Protection and Cybersecurity Law Review – 9th Edition. – 2022. [Электронный ресурс] - URL: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china (дата обращения: 05.11.2022).

[14] Платонова Н. И. Биометрические персональные данные: возможности и проблемы // Юрист. – 2019. – № 6. – с. 63-67.

Kazakhstan, a comprehensive legislative model has been adopted. Traditionally, legislation, such as the Decree of the Government of the Republic of Kazakhstan "On the approval of the Cybersecurity Concept ("Cybersecurity of Kazakhstan")"[15] dated June 30, 2017, No. 407, regulated the inclusion of personal biometric information in the category of personal information. Some other regulatory documents, such as the Law of the Republic of Kazakhstan "On Personal Data and their Protection"[16] dated May 21, 2013, No. 94-V and the Law of the Republic of Kazakhstan "On Informatization"[17] dated November 24, 2015, No. 418-V ZRK, also clarify the general rules for the protection of personal information and establish special rules for the protection of personal biometric information. In terms of legislative trends, the current drafts of the "Cybersecurity Concept" and the "Law on Personal Data and their Protection" have both entered the stage of public request for comments, and both have demonstrated a comprehensive legislative model. For example, the "Law on Personal Data and their Protection" jointly regulates important data and general data. At the same time, in comparison with a specialized legislative model, a comprehensive legislative model is more useful for solving the problems of decentralized legislation in Kazakhstan.

Firstly, the comprehensive legislative model has a clear level and a complete system. The protection of personal biometric information belongs to the branch of the legal system for the protection of personal information. A comprehensive legislative model may provide for special rules for the protection of personal biometric information, provided that the general rules for the protection of personal information are clarified, thereby ensuring the integrity of the legal system for the protection of personal information.[18] The second is complex methods of protection and protective measures of a comprehensive legislative model. On the one hand, the comprehensive legislative model is not limited to any one area, and it has universal applicability to the protection of personal biometric information. On the other hand, the methods of protection and protective measures are more comprehensive, including administrative protection, civil remedies and criminal sanctions.[19] Third, a comprehensive legislative model promotes the application of the law. The system of personal biometric information must not only comply with the basic principles and rules of the general collection, processing and use of personal information, but also comply with special rules of personal biometric information. A comprehensive legislative model helps to implement systemic coordination between general personal information and special personal biometric information, to avoid systemic violations caused by decentralized legislation, and to facilitate the application of the law. It should be noted that, on the one hand, faced with the current situation of abuse of personal biometric information, there is an urgent need for legislative protection. Especially before the security of Kazakhstan's biometric technologies was not fully confirmed, the risks of use were not fully assessed, and the protection mechanism was not yet systematized, personal biometric information was widely used, for example, not only in public scenarios such as national security and public security management, but also private scenarios such as finance, medical care, schools, payment, transportation, communities,

[15] Постановление Правительства Республики Казахстан «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)» от 30 июня 2017 года № 407 [Электронный ресурс] - URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 30.09.2022).

[16] Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V. [Электронный ресурс] - URL: https://adilet.zan.kz/rus/archive/docs/Z1300000094/14.07.2022 (дата обращения: 30.09.2022).

[17] Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК. [Электронный ресурс] - URL: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 30.09.2022).

[18] Victor Mayer-Schönberger/ Kenneth Cukier, Big Data John Murray 2013, 242 pages, ISBN 978-1-84854-792-6 [Электронный ресурс] - URL: https://www.jipitec.eu/issues/jipitec-5-1-2014/3912/jipitec_5_1_dreier.pdf (дата обращения: 06.11.2022).

[19] Pam Dixon. A Failure to "Do No Harm", Health Technol (Berl). 2017; 7(4): 539–567, Published online 2017 Jun 14. doi: 10.1007/s12553-017-0202-6 [Электронный ресурс] - URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5741784/# (дата обращения: 06.11.2022).

businesses, public property management, shopping malls, etc.[20]

The increasing use of biometric technologies has led to illegal trafficking and disclosure of personal biometric information in practice, violating the legitimate rights and interests of information subjects, such as privacy and property rights, and legislation and regulations are urgently needed. On the other hand, although the drafts of the "Cybersecurity Concept" and the "Informatization Law" have begun to be publicly requested for comments, biometric technologies have not yet been formed worldwide, and there is no consensus on the relevant technical standards, so it will take time to develop systematic, clear and complete rules regarding personal biometric information. Being a new problem in the era of big data, thoughtless legislation may prove counterproductive before mature practical experience in protecting personal biometric information is studied. Thus, faced with the problems of the current decentralized legislation of Kazakhstan on the protection of personal biometric information in combination with the current situation and trends in the development of information legislation of Kazakhstan, Kazakhstan should adopt a comprehensive legislative model. However, in order to address the current urgent need for personal biometric information to be protected by legislation, a model of "authorized legislation" and "local primary legislation" can be adopted to provide experience in formulating provisions on the protection of personal biometric information in comprehensive legislation. Thus, a progressive comprehensive legislative model is more suitable for Kazakhstan practice.

Kamalova G. G. in the monograph "Biometric personal data: definition and essence" also noted the inaccuracy of the norm-definition of biometric personal data.[21] In the modern Kazakh formulation of the definition of biometric personal data clearly insufficient behavioural traits. In this aspect, it seems appropriate to borrow from the foreign experience discussed above. At the same time, the definition enshrined in part 1 of Article 1 of the Law of the Republic of Kazakhstan No. 94-V "On personal data and their protection" of 21 May 2013, is often considered as satisfying the requirements of law enforcement practice. At the same time, the provisions of the legislation regulating the processing of biometric data currently do not take into account the use of modern digital technologies and technologies for processing genomic information.[22]

The legal regulation does not stipulate the roles, rights, duties and responsibilities of participants to regulate relations in the field of biometric identification, as well as their interaction.

In the Rules of classification of public services in electronic form to determine the method of authentication of the service recipient is not defined the possibility of authentication by means of a "Digital ID", despite the use of authentication in obtaining an electronic digital signature online.

There are no provisions in the legislation of Kazakhstan regarding the storage, collection and processing of biometric data used in the provision of public services. In addition, there is no right to "Digital footprint".

The fundamental principles governing legislation in the area of digital identification are based primarily on the protection of human rights and freedoms as well as citizens. Therefore, in order to ensure the protection of confidential information of personal data, legal norms, necessary amendments and additions to existing regulatory legal acts and interaction between existing and future mechanisms that do not contradict the Constitution of the Republic of Kazakhstan must be developed. Regulatory legal acts should contain provisions and regulations

[20] Ivan A. Tot, Jovan B. Bajčetić, Boriša Ž. Jovanović, Biometric standards and methods, Vojnotehnicki glasnik/ Military, Technical Courier, vol. 69, no. 4, pp. 963-977, 2021. [Электронный ресурс] - URL: https://www.redalyc.org/journal/6617/661770260009/html/ (дата обращения: 06.11.2022).

[21] Камалова Г.Г. Биометрические персональные данные: определение и сущность // Информационное право. – 2016. - № 3. – С. 8-12.

[22] Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V. [Электронный ресурс] - URL: https://adilet.zan.kz/rus/archive/docs/Z1300000094/14.07.2022 (дата обращения: 30.09.2022).

defining procedures, methods and mechanisms for the use and handling of biometric data of all modalities, delineation of responsibilities and regulatory areas of responsible authorities, interaction between current systems. Since the system affects the personal data of citizens of Kazakhstan and non-residents, the issue of personal data protection and liability for violation of the privacy of personal data should also be considered in regulatory legal acts.

Results

Based on the results of the conducted research of the models of legal regulation of biometric identification of individuals and legal entities existing in modern international law, in foreign jurisdictions, for the purposes of their legally significant actions in the field of public and private legal relations carried out through electronic services, as well as taking into account the analysis of the current legislation of the Republic of Kazakhstan in this area, the following are proposed offers:

The active use of systems using biometric data in the Republic of Kazakhstan should be accompanied by the provision of the necessary legal, procedural, and technical guarantees to protect against unauthorized access by third parties to databases, fraudulent transactions to personal data.

At the legislative level, the State needs to regularly review the provisions and regulations relating to the protection of personal data. Because the provisions and regulations must continue to be relevant to the emerging risks posed by the rapid development and enhancement of biometric technologies.

Conclusion

In the era of modern digital technologies, the existing security risks in biometric authentication are quite serious. Consequently, interested parties need to respond promptly to the latest developments so that the data of individuals and legal entities can be reliably protected.

In this regard, at the legislative level, all conditions of protection should be clearly defined and regulated. They should also be aimed at the ability of users to control their biometric data.

We propose the following amendments and additions to the legislation of the Republic of Kazakhstan:

- to amend the current legislation of the Republic of Kazakhstan regulating civil and public legal relations in the form of electronic interaction, in terms of defining terminology in the field of personal data identification and the formation of a unified terminology base. Moreover, the improvement of the institute of legal regulation of identification and authentication technologies based on biometric data.

- to develop provisions aimed at establishing the possibility of working with electronic documents signed by an analogue of the client's handwritten signature on an electronic tablet, in particular, regulating the process of obtaining a sample of a handwritten signature, digitizing it and comparing the electronic analogue of a handwritten signature with an existing sample.

References

1. Kukharev G. A. Biometricheskie sistemy: Metody i sredstva identifikatsii lichnosti cheloveka [Biometric systems: Methods and means of identification of a person], Politekhnika. pp. 240. (2001). [in Russian]

2. Afanas'ev A. A. Autentifikatsiya. Teoriya i praktika obespecheniya bezopasnogo dostupa k informatsionnym resursam [Authentication. Theory and practice of providing secure access to information resources], Uchebnoe posobie dlya vuzov: Grif UMO MO RF, Goryachaya liniya, Telekom, pp. 254. (2012). [in Russian]

3. Barry, A. Ireland 'should consider laws that would jail cyber bullies' (TheJournal.ie. 2013). [Electronic resource] – Available at: https://www.thejournal.ie/cyber-bullying-ireland-1162881-Nov2013/ (Accessed: 03.09.2022).

4. Gomez-Barrero M., Drozdowski P. Biometrics: Challenges and Opportunities (IEEE Transactions on Technology and Society, 2022). [Electronic resource] – Available at: https://arxiv.org/pdf/2102.09258 (Accessed: 04.09.2022).

5. Ben-Shahar O, Jacob L. S. Confidentiality Agreements: An Introduction [J], Journal of Legal Studies 2016 (2), pp. 51–61.

6. William Fry and Forbes. Europe for Big Data (Forbes Insights, 2016). [Electronic resource] – Available at: http://www.williamfry.com/docs/defaultsource/reports/william-fry-europe-for-big-data-report.pdf?sfvrsn=0 (Accessed: 05.09.2022).

7. Custers B., Van der Hof S., Schermer B., Appleby-Arnold S., and Brockdorff N. Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law (SCRIPTed, Journal of Law, 2013, Technology and Society, Volume 10, Issue 4, pp. 435–457). [Electronic resource] – Available at: https://script-ed.org/article/informed-consent-social-media-gap-user-expectations-eu-personal-data-protection-law/ (Accessed: 07.09.2022).

8. Mason S. Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation (SCRIPTed, Journal of Law, 2012, Technology and Society, Volume 9, Issue 1, p. 327). [Electronic resource] – Available at: https://script-ed.org/article/informal-debate-on-the-issues-relating-to-terminology-and-clarification-of-concept-in-respect-of-the-eu-e-signature-legislation/ (Accessed: 06.09.2022).

9. Report of Secure Identity Alliance & the onepoint team "Giving Voice to Digital Identities Worldwide - Key insights and experiences to overcome shared challenges", 2021. [Electronic resource] – Available at: https://secureidentityalliance.org/publications-docman/public/163-21-02-12-giving-voice-to-digital-identities-worldwide-en/file (Accessed: 07.09.2022).

10. Vecchi D. and Marchese M. Italy: The Privacy, Data Protection and Cybersecurity Law Review (Law Business Research. – Chapter 15, 9th Edition, 2021). [Electronic resource] – Available at: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review (Accessed: 08.09.2022).

11. See List of acceptable supporting documents for verification (July 01, 2022) [Electronic resource] – Available at: https://uidai.gov.in/images/commdoc/valid_documents_list.pdf (Accessed: 11.09.2022).

12. Dar A., Viswanath N., Suri Sh. The Financial Technology Law Review: India (The Law Reviews, 5th Edition, 2022). [Electronic resource] – Available at: https://thelawreviews.co.uk/title/the-financial-technology-law-review/india (Accessed: 11.10.2022).

13. Yang H. The Privacy, Data Protection and Cybersecurity Law Review: China (The Privacy, Data Protection and Cybersecurity Law Review, 9th Edition, 2022). [Electronic resource] – Available at: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china (Accessed: 05.11.2022).

14. Platonova N. I. Biometricheskie personal'nye dannye: vozmozhnosti i problem [Biometric personal data: opportunities and problems], Yurist. No 6. pp. 63-67. (2019). [in Russian]

15. Resolution of the Government of the Republic of Kazakhstan «On approval of the Cybersecurity Concept («Cybersecurity of Kazakhstan»)» dated June 30, 2017 No. 407 [Electronic resource] – Available at: https://adilet.zan.kz/rus/docs/P1700000407 (Accessed: 30.09.2022).

16. Zakon Respubliki Kazakhstan «O personal'nykh dannykh i ikh zashchite» ot 21 maya 2013 goda № 94-V. [The Law of the Republic of Kazakhstan «On Personal Data and their protection» dated May 21, 2013 No. 94-V.] [Electronic resource] – Available at: https://adilet.zan.kz/rus/archive/docs/Z1300000094/14.07.2022 (Accessed: 30.09.2022).

17. Law of the Republic of Kazakhstan «On informatization» dated 24 November 2015 № 418-V. [Electronic resource] – Available at: https://adilet.zan.kz/rus/docs/Z1500000418 (Accessed: 30.09.2022).

18. Victor Mayer-Schönberger/ Kenneth Cukier, Big Data John Murray 2013, 242 pages, ISBN 978-1-84854-792-6 [Электронный ресурс] - URL: https://www.jipitec.eu/issues/jipitec-5-1-2014/3912/jipitec_5_1_dreier.pdf (дата обращения: 06.11.2022).

19. Pam Dixon. A Failure to "Do No Harm", Health Technol (Berl). 2017; 7(4): 539–567, Published online 2017 Jun 14. doi: 10.1007/s12553-017-0202-6 [Электронный ресурс] - URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5741784/# (дата обращения: 06.11.2022).

20. Ivan A. Tot, Jovan B. Bajčetić, Boriša Ž. Jovanović, Biometric standards and methods, Vojnotehnicki glasnik/Military, Technical Courier, vol. 69, no. 4, pp. 963-977, 2021. [Электронный ресурс] - URL: https://www.redalyc.org/journal/6617/661770260009/html/ (дата обращения: 06.11.2022).

21. Kamalova G.G. Biometricheskie personal'nye dannye: opredelenie i sushchnost' [Biometric personal data: definition and essence], Informatsionnoe pravo. No 3. pp. 8-12. (2016). [in Russian]

22. Zakon Respubliki Kazakhstan «O personal'nykh dannykh i ikh zashchite» ot 21 maya 2013 goda № 94-V. [The Law of the Republic of Kazakhstan «On Personal Data and their protection» dated May 21, 2013 No. 94-V.] [Electronic resource] – Available at: https://adilet.zan.kz/rus/archive/docs/Z1300000094/14.07.2022 (Accessed: 30.09.2022).

Ж.Т. Искакова, Т.С. Қадыржанова
Евразийский национальный университет имени Л.Н. Гумилева, Астана, Казахстан

Анализ проблем и вызовов в законодательстве Республики Казахстан по защите персональных данных и международно-правовое регулирование

Аннотация. Авторами проводится анализ международно-правового и национально-правового регулирования с целью изучения, определения уровня нормативной защищенности идентификации и аутентификации физических и юридических лиц для целей совершения ими юридически значимых действий в различных сферах общественных отношений в Республике Казахстан.

Предпринята попытка сформулировать определённые выводы и предложения, которые, с одной стороны, предоставят возможность государству обеспечить уровень доверия граждан, юридических лиц в сфере электронного информационного взаимодействия, с другой - уменьшать риски, связанные с утечками баз биометрических данных пользователей информационных систем, и не нарушать конфиденциальности биометрических персональных данных физических и юридических лиц, а также повысить эффективность в сфере публично-правовых и частно-правовых взаимоотношений, осуществляемых посредством электронных сервисов.

Ключевые слова: биометрия, биометрические данные, персональные данные, биометрическая идентификация, цифровая идентификация, аутентификация, GDPR.

Ж.Т. Искакова, Т.С. Қадыржанова
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

Қазақстан Республикасының дербес деректерді қорғау жөніндегі заңнамасындағы проблемалар мен сын-қатерлерді талдау және халықаралық-құқықтық реттеу

Аңдатпа. Авторлар Қазақстан Республикасындағы қоғамдық қатынастардың түрлі салаларында заңи маңызы бар іс-әрекеттер жүргізу мақсатында жеке және заңды тұлғаларды идентификациялау мен аутентификациялаудың нормативті қорғалу деңгейін зерделеу, айқындау мақсатында халықаралық-құқықтық және ұлттық-құқықтық реттеуге талдау жүргізеді.

Авторлар белгілі бір тұжырымдар мен ұсыныстарды тұжырымдауға тырысты. Бір жағынан, осы тұжырымдалған ұсынымдар мемлекетке азаматтар мен заңды тұлғалардың электрондық ақпараттық өзара іс-қимыл саласындағы сенім деңгейін қамтамасыз етуге мүмкіндік береді. Екінші жағынан, дәл осындай ұсыныстар ақпараттық жүйелерді пайдаланушылардың биометриялық дерекқорларының таралып кетуімен байланысты тәуекелдерді азайтады, сонымен қатар, жеке және заңды тұлғалардың биометриялық дербес деректерінің құпиялылығын сақтауға ықпал етеді. Сондай-ақ, ұсынымдар электрондық сервистердің көмегімен жүзеге асырылатын жария-құқықтық және жеке-құқықтық қатынастар саласындағы тиімділікті арттыруға бағытталған.

Түйін сөздер: биометрия, биометриялық деректер, дербес деректер, биометриялық идентификациялау, цифрлық идентификациялау, аутентификациялау, GDPR.

Список литературы

1. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека // Политехника. – 2001. – с. 240.

2. Афанасьев А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам // Учебное пособие для вузов. – Гриф УМО МО РФ. – Горячая линия - Телеком, 2012. – с. 254.

3. Barry, A. Ireland 'should consider laws that would jail cyber bullies' // TheJournal.ie. – 2013. [Электронный ресурс] - URL: https://www.thejournal.ie/cyber-bullying-ireland-1162881-Nov2013/ (дата обращения: 03.09.2022).

4. Gomez-Barrero M., Drozdowski P. Biometrics: Challenges and Opportunities // IEEE Transactions on Technology and Society. – 2022. [Электронный ресурс] - URL: https://arxiv.org/pdf/2102.09258 (дата обращения: 04.09.2022).

5. Ben-Shahar O, Jacob L. S. Confidentiality Agreements: An Introduction [J], Journal of Legal Studies 2016 (2), pp. 51–61.

6. William Fry and Forbes. Europe for Big Data // Forbes Insights, 2016. [Электронный ресурс] - URL: http://www.williamfry.com/docs/defaultsource/reports/william-fry-europe-for-big-data-report.pdf?sfvrsn=0 (дата обращения: 05.09.2022).

7. Custers B., Van der Hof S., Schermer B., Appleby-Arnold S., and Brockdorff N. Informed Consent in Social Media Use. The Gap between User Expectations and EU Personal Data Protection Law // SCRIPTed, Journal of Law, 2013, Technology and Society, Volume 10, Issue 4, pp. 435–457. [Электронный ресурс] – URL: https://script-ed.org/article/informed-consent-social-media-gap-user-expectations-eu-personal-data-protection-law/ (дата обращения: 07.09.2022).

8. Mason S. Informal Debate on the Issues Relating to Terminology and Clarification of Concept in Respect of the EU e-Signature Legislation // SCRIPTed, Journal of Law, 2012, Technology and Society, Volume 9, Issue 1, p. 327. [Электронный ресурс] – URL: https://script-ed.org/article/informal-debate-on-the-issues-relating-to-terminology-and-clarification-of-concept-in-respect-of-the-eu-e-signature-legislation/ (дата обращения: 06.09.2022).

9. Отчет Secure Identity Alliance & the onepoint team "Giving Voice to Digital Identities Worldwide - Key insights and experiences to overcome shared challenges", 2021. [Электронный ресурс] – URL: https://secureidentityalliance.org/publications-docman/public/163-21-02-12-giving-voice-to-digital-identities-worldwide-en/file (дата обращения: 07.09.2022).

10. Vecchi D. and Marchese M. Italy: The Privacy, Data Protection and Cybersecurity Law Review // Law Business Research. – Chapter 15, 9th Edition, 2021. [Электронный ресурс] – URL: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review (дата обращения: 08.09.2022).

11. См.: List of acceptable supporting documents for verification. 01 июля 2022 года. [Электронный ресурс] - URL: https://uidai.gov.in/images/commdoc/valid_documents_list.pdf (дата обращения: 11.09.2022).

12. Dar A., Viswanath N., Suri Sh. The Financial Technology Law Review: India // The Law Reviews – 5th Edition. – 2022. [Электронный ресурс] - URL: https://thelawreviews.co.uk/title/the-financial-technology-law-review/india (дата обращения: 11.10.2022).

13. Yang H. The Privacy, Data Protection and Cybersecurity Law Review: China // The Privacy, Data Protection and Cybersecurity Law Review – 9th Edition. – 2022. [Электронный ресурс] - URL: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/china (дата обращения: 05.11.2022).

14. Платонова Н. И. Биометрические персональные данные: возможности и проблемы // Юрист. – 2019. – № 6. – с. 63-67.

15. Постановление Правительства Республики Казахстан «Об утверждении Концепции кибербезопасности («Киберщит Казахстана»)» от 30 июня 2017 года № 407 [Электронный ресурс] - URL: https://adilet.zan.kz/rus/docs/P1700000407 (дата обращения: 30.09.2022).

16. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V. [Электронный ресурс] - URL: https://adilet.zan.kz/rus/archive/docs/Z1300000094/14.07.2022 (дата обращения: 30.09.2022).

17. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК. [Электронный ресурс] - URL: https://adilet.zan.kz/rus/docs/Z1500000418 (дата обращения: 30.09.2022).

18. Victor Mayer-Schönberger/ Kenneth Cukier, Big Data John Murray 2013, 242 pages, ISBN 978-1-84854-792-6 [Электронный ресурс] - URL: https://www.jipitec.eu/issues/jipitec-5-1-2014/3912/jipitec_5_1_dreier.pdf (дата обращения: 06.11.2022).

19. Pam Dixon. A Failure to "Do No Harm", Health Technol (Berl). 2017; 7(4): 539–567, Published online 2017 Jun 14. doi: 10.1007/s12553-017-0202-6 [Электронный ресурс] - URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5741784/# (дата обращения: 06.11.2022).

20. Ivan A. Tot, Jovan B. Bajčetić, Boriša Ž. Jovanović, Biometric standards and methods, Vojnotehnicki glasnik/Military, Technical Courier, vol. 69, no. 4, pp. 963-977, 2021. [Электронный ресурс] - URL: https://www.redalyc.org/journal/6617/661770260009/html/ (дата обращения: 06.11.2022).

21. Камалова Г.Г. Биометрические персональные данные: определение и сущность // Информационное право. – 2016. - № 3. – С. 8-12.

22. Закон Республики Казахстан «О персональных данных и их защите» от 21 мая 2013 года № 94-V. [Электронный ресурс] - URL: https://adilet.zan.kz/rus/archive/docs/Z1300000094/14.07.2022 (дата обращения: 30.09.2022).

Сведения об авторах:

Қадыржанова Т.С. **– негізгі автор,** *Л*.Н.Гумилев атындағы Еуразия ұлттық университеті «Халықаралық құқық» кафедрасының магистранты, Астана, Қазақстан.

Искакова Ж.Т. – доктор PhD, *Л*.Н.Гумилев атындағы Еуразия ұлттық университеті «Халықаралық құқық» кафедрасының доцент міндетін атқарушы, Астана, Қазақстан.

Kadyrzhanova T.S. – **The main author,** Master's student in the International Law Department, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan.

Iskakova Zh.T. – Ph.D., Acting Assistant Professor in the International Law Department, L. N. Gumilyov Eurasian National University, Astana, Kazakhstan.