Л.Н. Гумилев атындағы Еуразия ұлттық университетінің ХАБАРШЫСЫ.
ISSN: 2616-6844. eISSN: 2663-1318

ҚҰҚЫҚ СЕРИЯСЫ/ LAW SERIES/ СЕРИЯ ПРАВО

Азаматтық құқық. Азаматтық процесс / Civil law. Civil process / Гражданское право. Гражданский процесс

IRSTI 10.19.61 https://doi.org/10.32523/2616-6844-2025-153-4-57-75
Scientific article

Legal Problems of Protecting Personal Data of Citizens in the Republic of Kazakhstan

T.S. Tilep*[1], E. Juchnevicius[2]

[1]*Buketov Karaganda National Research University, Karaganda, Kazakhstan*
[2]*University of Gdańsk, Gdańsk, Poland*

(e-mail: tlep97@mail.ru[1], e.juchnevicius@prawo.ug.edu.pl[2])

Abstract: The article examines the current state of legislation governing the protection of personal data, the challenges arising in its implementation, and the prospects for improving the protection mechanism through the use of blockchain technology. Frequent cases of unlawful dissemination of personal data in Kazakhstan are directly linked to unresolved issue of cybersecurity and the need to address vulnerabilities in the existing legislation, which underscores the relevance of the chosen research topic. The purpose of this study is to establish a legal framework for the protection and security of personal data through the use of digital technologies. The scientific novelty of this work lies in the fact that, for the first time since the formation of the legislative framework governing personal data in the Republic of Kazakhstan, legal norms regarding personal data have been defined, as well as areas of legal regulation for the circulation of certain types of personal data. Measures to improve existing legislation governing the circulation of personal data have been proposed. The above constitutes a national scientific doctrine in the field of personal data protection. New practical conclusions have been summarized, allowing for the improvement of existing national legislation and, consequently, their application in legislative activity. The research methods used include a general logical approach (induction, deduction), systematization, analysis, formulation, scientific methods, and empirical methods.

Ensuring the security of personal data is a state obligation arising from the duty to protect individual human rights; therefore, the authors emphasize the particular importance of strengthening control over digital threats and introducing a procedure for assessing their impact on human rights in accordance with international standards. The study concludes that the Republic of Kazakhstan should accede to international instruments establishing standards for the protection of personal data. A potential pathway for strengthening the legal framework on personal data protection lies in establishing systemic safeguards that restrict unauthorized access to information. Such mechanisms should operate across all levels of data governance, ensuring consistent compliance among data holders, processors and supervisory entities. Based on the results of the research, it is proposed to adopt a legal norm regulating continuous control and monitoring by data owners, operators, and persons responsible for organizing the processing and storage of personal data.

Keywords: digitalization, Digital Code, personal data, biometric data, identification, personal data protection, cybersecurity.

Received: 07.11.2025. Accepted: 19.12.2025. Available online: 30.12.2025

***the corresponding author**

Introduction

In Kazakhstan, the process of digitalization and information processing is developing intensively. One of the priorities of the National Development Plan of the Republic of Kazakhstan until 2029 is the optimization of regulation aimed at supporting innovation, as well as the digital and creative economy. The second strategic direction of the National Development Plan highlights that improving regulatory procedures in the sphere of personal data governance should decrease the likelihood of information breaches, enhance operational reliability, and reinforce public and investor confidence in Kazakhstan's digital infrastructure. It also underscores the necessity of strengthening the accountability of data controllers who infringe upon citizens' rights to informational privacy and of establishing preventive mechanisms for identifying and mitigating data leaks, including timely notification of affected individuals [1]. The practical implementation of this state program presupposes a complex set of actions, foremost among which is the modernization of cybersecurity legislation and the establishment of an integrated framework for legal and technological protection.

The second strategic direction priority emphasizes that «the optimization of regulation in the field of personal data protection will reduce the risk of data leakage, increase the reliability of operations, and strengthen the confidence of investors, businesses, and citizens in Kazakhstan's digital ecosystem. In addition, it is envisaged to tighten the liability of operators who have violated the rights of other citizens to the protection of personal data, as well as to develop mechanisms for detecting and preventing data leaks, including notifying data owners».

The implementation of the National Development Plan requires the application of comprehensive measures, beginning with the improvement of legal regulation in the field of cybersecurity.

The establishment of e-government has influenced not only the transformation of relations between the state and society but has also contributed to the reduction of budgetary expenditures. However, alongside these positive developments in Kazakhstan's information space, there is a growing trend of risks and threats in the field of information security.

The relevance of the topic is determined by the aggravation of the problem of ensuring the security of digital data in Kazakhstan. Insufficient protection of personal data has led to information leaks, as a result of which citizens increasingly become victims of fraud. Citizens are deceived over the phone, and numerous loans are fraudulently registered in their names. Given the limited effectiveness of current law enforcement measures against cybercrime, the challenge of ensuring secure storage and protection of personal data continues to be a critical concern. Multiple high-profile breaches demonstrate persistent vulnerabilities within national information systems. A notable example is the recent revelation of unauthorized access to databases containing personal details of Kazakhstani citizens, which subsequently appeared on various social media platforms.

According to the Department for Combating Cybercrime of the Ministry of Internal Affairs of the Republic of Kazakhstan, more than forty cases of data leaks have been recorded since the beginning of 2025. Instances have been identified where employees of private organizations, having access to such data, sold them for remuneration [2]. It has also been reported that this data is currently being sold on closed Telegram channels.

In June of the current year, the leakage of personal data of more than sixteen million Kazakhstani citizens caused a wide public outcry and heightened public concern. Assuming

that each record corresponds to one individual, it can be stated that the data of approximately 70 percent of the country's population became publicly accessible [3].

The published data included the surname, first name, patronymic, gender, date of birth, individual identification number (IIN), address, date of residence registration, mobile, home, and work telephone numbers, citizenship, nationality, and other personal information [4].

In his recent Address to the Nation, the President of the Republic of Kazakhstan set forth the task of entering the era of universal digitalization and artificial intelligence, as well as transforming Kazakhstan into a full-fledged digital state [5].

President Kassym-Jomart Tokayev emphasized that emerging technologies also bring significant threats: artificial intelligence systems are capable of generating biometric imitations of people, reproducing their likeness through synthesized voice, visual, or behavioral patterns. Such capabilities, he warned, could compromise personal data and financial security, while also enabling the spread of fabricated media aimed at influencing public perception [6].

The dissemination of data increases the risks of fraud. Criminals may launch cyberattacks on the eGov system, target banks, or contact clients with fraudulent offers.

The right to privacy contributes to the development of other human and civil rights and freedoms, to the creative development of the individual, and to the democratization of society. Therefore, the proclamation of the right to «privacy, personal and family secrecy» as one of the fundamental human rights, and the establishment of legal guarantees for its observance, constitute one of the key functions of the Constitution of the Republic of Kazakhstan.

The purpose of this research is to provide a comprehensive understanding of the concept and classification of personal data, to conduct a comparative legal analysis of international instruments and national legislation governing their legal regulation, and to develop recommendations aimed at improving the mechanisms for the protection of personal data.

In order to realize the stated research goal, several specific objectives have been formulated. First, the study seeks to conduct a detailed examination of incidents involving breaches and improper handling of personal data. Second, it aims to clarify the theoretical foundations of the concept of personal data identifying its essential characteristics, structural elements, and key classifications. Third, the research proposes a set of recommendations designed to enhance citizens' ability to manage digital data and to secure their legal rights to supervise and erase such information within the framework of national legislation. Fourth, it seeks to determine effective mechanisms for the incorporation of international legal norms into the domestic legal system. Finally, the study explores the potential application of modern digital technologies that can ensure the reliable protection and long-term security of personal data.

To date, no fundamental scientific research has been conducted in Kazakhstan on the topic under consideration, and it has not been the subject of specialized academic study, since no monographic works have been published on this issue. The content of the existing articles is informational in nature; the problems raised in them are treated superficially and limited to a general analysis. The number of academic studies conducted within this topic is limited. Among the scholars who have contributed to the study of this topic are Russian researchers such as Sokolova O.S., Travkin Yu., Chernyaeva D.V., and others, as well as Kazakhstani researchers including Suleimenov M.K., Nesterova E.V., Ilyassova G.A., Aitimov B.Zh., Zhamburbayeva S., Turysbekuly M., and Tokatov R.A.

Scientific novelty. For the first time, this study develops scientifically grounded proposals to improve national legislation aimed at ensuring the protection of personal data through the

use of blockchain technology. The study proposes ways to enhance the legal mechanisms for regulating the protection of personal data.

Materials and Methods

In the process of writing this article, a combination of deductive and inductive methods is used, allowing the research to move from the analysis of specific legal issues to broader generalizations. This methodological approach makes it possible to refine existing mechanisms for the legal protection of personal data to substantiate the economic and legal prerequisites for the use of blockchain technology.

Special attention is paid to analytical and systematization methods, which are used to identify the key elements of the research object and to examine the interconnections between them. This approach enables a comprehensive assessment of the challenges with which the Republic of Kazakhstan is faced, including issues related to the unlawful dissemination of personal data and the insufficient level of digital culture in society. Blockchain technology is not considered in isolation, but as part of an integrated legal and socio-economic system, whose elements continuously interact and influence one another.

The study is based on a clearly defined conceptual framework, which determines the main directions, priorities and methodological approaches of the research. The scientific method relies on established doctrines and scholarly findings, uses recognized scientific categories, and is also oriented towards achieving concrete research objectives rather than a purely descriptive analysis.

Comparative legal analysis is applied to examine international experience in regulating personal data protection mechanisms. The results of this comparison serve as a basis for developing proposals aimed at improving national-level regulation, taking into account both foreign best practices and domestic legal realities.

At the same time, the formal legal method is used selectively, primarily for the analysis of cases concerning the protection of citizens' personal data and instances of violations of personal data legislation. This allows the study to assess not only the normative order of regulation, but also its practical implementation.

To evaluate the effectiveness of existing legal mechanisms for personal data protection in the Republic of Kazakhstan, statistical and descriptive analytical methods are employed. In addition, advanced international experience in the application of blockchain technology is analyzed in order to determine the feasibility and potential effectiveness of its use for the development of the national economy.

The empirical component of the research draws on previously conducted studies as well as the author's own academic experience, which provides an additional practical dimension to the analysis.

In the process of preparing the article, statutory and regulatory acts were examined, relevant legal scholarship was analyzed, statistical data and electronic information resources were processed, which ensured the reliability and completeness of the findings.

The following documents were used in the process of writing the article: the Law of the Republic of Kazakhstan «On Personal Data and Their Protection» No. 94-V dated May 21, 2013; the Law of the Republic of Kazakhstan «On State Secrets» No. 349-I dated March 15, 1999; the Law of the Republic of Kazakhstan «On Informatization» No. 418-V dated November 24, 2015;

ETS Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (Strasbourg, January 28, 1981); General Data Protection Regulation (GDPR) of the European Union of 2016; analysis of sources in legal literature, statistical indicators and processing of electronic information.

Results and Discussion

In the modern world, it is generally impossible to completely eliminate the possibility of identifying an individual; however, it is both possible and necessary to prohibit the storage, processing, and use of personal information without the consent of its subject. Measures to ensure the security of personal data and to prevent unlawful actions have acquired legal expression in the form of the concept of personal data protection. Although its foundations were established through foreign experience, Kazakhstan has successfully adopted them, taking into account not only the accumulated legal practices of foreign states but also the political transformations within Kazakhstani society, social realities, and contemporary trends in the development of law.

The adoption of the Law of the Republic of Kazakhstan «On Personal Data and Their Protection» (No. 94-V, 21 May 2013) marked an important step in forming the foundations of cross-sectoral regulation of relations arising in the field of personal data circulation. Today, within the Kazakhstani system of personal data regulation, three key areas are developing successfully:

a) the formation of a comprehensive body of legislation aimed at regulating the circulation of personal data;

b) the establishment of specific principles for handling personal data, consistently enshrined in normative acts of various levels;

c) the creation of a special institutional framework ensuring oversight of the observance of the rights of personal data subjects.

However, the process of developing a regulatory framework governing the circulation of personal data, in our view, still remains at a formative stage, which is primarily evidenced by the active legislative activity in this field.

As defined in the Law of the Republic of Kazakhstan «On Personal Data and Their Protection» (No. 94-V, 21 May 2013), Article 1 establishes that personal data comprise any information referring to an individual who is identified or can be identified, and such data may exist in electronic, paper, or other material form [7]. The same provision also specifies that biometric data represent a distinct subset of personal data, reflecting a person's physiological and biological characteristics that allow for their identification [7]. Such biometric data include an individual's facial image, fingerprints, genomic information, and other similar identifiers.

In the context of identification information, this group encompasses data elements such as document numbers verifying an individual's legal or civil status – including identity cards, passports, birth certificates, and educational diplomas – alongside personal identifiers like the individual identification number (IIN) and biometric attributes. At present, centralized automated databases are being created in Kazakhstan. However, as recent events have demonstrated, the level of their protection against cyberattacks remains extremely low. In certain cases, the unlawful dissemination of personal data has resulted from the actions of public officials themselves. Some information relating to citizens' personal data is, in fact, not subject

to protection at all. For instance, there currently exist Telegram bots that allow the identification of an individual by their IIN. A similar situation is observed with vehicle registration numbers, for which there is no explicit legal prohibition on dissemination. Meanwhile, the increase in criminal activity associated with fraud in large cities is largely due to the uncontrolled use of such information.

The legislation of the European Union maintains a clear and consistent position on this matter. The Directive of the European Parliament and of the Council of the European Union «Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector» (No. 2002/58/EC) (12 July 2002) (GDPR) states that «information relating to subscribers of publicly available telecommunications systems contains data concerning the privacy of individuals» [8]. In particular, under this document, citizens are granted the so-called «right to be forgotten», which entitles them to request the deletion of their personal data.

The next block of information belonging to the category of personal privacy consists of biographical data that describes an individual's life path. If access to identification data is regulated by normative legal acts through the method of prohibition, biographical information may be collected, stored, and disseminated exclusively with the consent of the citizen – that is, it is protected by means of authorization. Information on whether an individual has previously been subjected to criminal liability and on the completion or serving of a sentence may be disclosed only within the competence of state authorities. Furthermore, questions concerning criminal records should be excluded from questionnaires completed during employment procedures.

The next group of data falling within the category of personal privacy comprises information on an individual's family status. At first glance, this category of personal data may appear to constitute part of biographical information and not to belong to confidential data. However, such information includes data constituting the secrecy of adoption, information on marriage or divorce, children born out of wedlock, and details regarding alimony obligations. All these elements form part of an individual's informational portrait – aspects that a person may wish not to disclose. Therefore, such information must be protected by official authorities and should not be publicly accessible. Consequently, information regarding an individual's family status may rightfully be classified as personal data.

Since information about a citizen's family status constitutes a legally protected personal secret, such data, in our view, must be subject to enhanced legal protection. The secrecy of child adoption, details of marriage or divorce, obligations to pay alimony, as well as information about children born out of wedlock, are strictly personal and therefore should not be publicly accessible. Given that data concerning the family status of citizens are classified as personal data, the state must ensure their proper and reliable protection.

Another type of data comprising personal information is information on an individual's social status. Market relations have contributed to the stratification of the population by property status, which in turn has generated other forms of social differentiation. If the goal of the state is the construction of a civil society, then the legal division of citizens into social groups is inadmissible. Therefore, questions concerning social status (for example, family, material, orphan, large family, disability status, etc.) should be excluded from most questionnaires and survey forms. The decision to provide such information must be made by the citizen personally, and if such data are provided, the procedures for their collection, storage, and protection must be clearly defined.

The next group of personal data that deserves particular attention is information characterizing an individual's financial status. With the development of market relations, the relevance of protecting this category of information has significantly increased. There are several reasons for this. First, a person's financial (property) status largely determines their social position. Second, even lawfully obtained information, if disclosed without the individual's consent, may become the subject of discussion among various groups and result in financial difficulties. Third, many public authorities attempt to collect unjustified information concerning the financial situation of citizens.

Medical information relating to a natural person requires a special regime of protection. The issues of securing information systems in the field of healthcare that contain personal medical data, ensuring their integrity and confidentiality, the patient's right to access their own medical data, as well as the obligation to inform citizens when such information is requested, are regulated by the Code of the Republic of Kazakhstan «On the Health of the People and the Healthcare System» (No. 360-VI, 7 July 2020).

In our view, this category represents one of the most protected types of personal data. Beyond data on an individual's physical and mental health, medical records should also encompass relevant information about the health condition of immediate family members. The availability of precise and trustworthy medical data serves as a key prerequisite for making objective diagnoses and choosing the most appropriate therapeutic strategies. Such information must be maintained exclusively within the confidential framework of the «patient-physician» relationship and may only be shared with third parties upon the patient's explicit consent, or, when the patient is unable to make an informed decision, with the authorization of close relatives or legal guardians.

To gain a deeper understanding of the nature and essence of the category under consideration, it is necessary to distinguish between the concepts of «health status» and «medical information relating to an individual» [9]. The term «medical information relating to an individual» refers to a set of data concerning past illnesses, the presence of diseases, their progression, applied methods of treatment and medicinal products, prognosis, and other similar information. The concept of «health status', in accordance with subparagraph 11 of paragraph 14 of Article 1 of the Law of the Republic of Kazakhstan «On State Secrets» (No. 349-1, 15 March 1999), encompasses general information regarding an individual's illnesses and correlates such information with the person's ability to perform official duties, based on the overall condition of the body [10]. A citizen holding a high-ranking state position has the right to demand compliance with the regime of medical confidentiality, provided that they fully perform official duties. However, maintaining the regime of state secrecy with respect to such information may lead to adverse consequences for the future of the country. Therefore, the protection of medical information relating to an individual requires the development of mechanisms distinct from those ensuring the protection of state secrets.

In recent years, society has shown particular interest in a category of personal privacy associated with the characteristics of citizens' sexual life and their sexual orientation. This category of personal data has a distinctly individual nature and has traditionally been subject to strict confidentiality. Therefore, the right to collect and process such information should be maximally restricted. If such data becomes known to medical professionals for any reason, they must be isolated from the general category of personal data – they should not be included in

the medical record and may be transferred from one physician to another only with the explicit consent of the patient.

The current legislation divides personal data by the level of accessibility in to «publicly available» and «restricted-access data» [11].

According to the law, personal data to which the confidentiality requirements established by the legislation of the Republic of Kazakhstan do not apply are considered publicly available. However, even in such cases, access to these data is permitted only with the consent of the data subject. The consent of the data subject may be formalized in written form, in an electronic document, or by other means that make it possible to confirm consent through the use of an electronic digital signature. It can therefore be concluded that the data subject independently defines the category under which their personal information falls, depending on the purpose of its collection and the extent to which such data is required. In accordance with current legislation, if an individual considers that the acquisition or processing of their personal information has taken place in breach of legal norms, they are entitled to petition the competent public authority or initiate judicial proceedings seeking the deletion of this information from open-access databases. Should the request be approved by the relevant authority, the decision must be executed within one working day.

Personal data is stored in databases located on the territory of the data owner (operator) or third parties. They may be used solely for the purposes specified in the initial request and may be disseminated only if such dissemination does not infringe upon the rights and freedoms of the data subject or prejudice the legitimate interests of other natural or legal persons.

The dissemination of personal data beyond the declared purposes is permissible only with the consent of the data subject or their legal representative. The protection of personal data is understood as a set of measures aimed at preventing unauthorized disclosure, use, alteration, or destruction of such data without the consent of their owner, as well as at ensuring the prevention of potential violations in this field.

Under subparagraph 1, paragraph 1 of Article 1 of the Law of the Republic of Kazakhstan On Personal Data and Their Protection (21 May 2013), biometric data are defined as personal information reflecting the physiological and biological traits of an individual, which allow that person to be identified or authenticated [11]. This category encompasses such identifiers as facial geometry, fingerprint patterns, vocal characteristics, iris configuration, DNA profiles, and other physiological or biological indicators capable of confirming or verifying a person's identity [11]. Such biometric data include a person's facial features, fingerprints, voice, iris pattern, DNA analysis results, as well as other physiological and biological characteristics that enable the identification or verification of an individual's identity.

In recent years, biometric data have been increasingly used in emerging technologies based on their recognition and application. For example, voice is used in «smart home» systems, while fingerprints, facial images, and iris patterns are employed for accessing personal accounts and unlocking mobile devices. Technologies utilizing the geometry of the palm, iris scans, and even human DNA are also in active use.

However, a facial image is not recognized as personal data in all cases. The Kazakhstani legal scholar Turysbekuly M. provided a clear interpretation of this issue, noting that a digital photograph or video recording of a person collected for identification purposes constitutes personal data [12].

Public debates concerning the potential abuse of authority by the state and law enforcement agencies in ensuring the security of citizens' fingerprint information have continued within society. «In our case, the risk of unlawful use of fingerprints always exists. In certain situations, data may be sold or powers may be abused, given the low level of public trust in law enforcement agencies», says Zhovtis E., Director of the Kazakhstan International Bureau for Human Rights and Rule of Law [13]. Some experts believe that biometric data can be forged, thereby creating risks of identity substitution or passport falsification. «If such data are stolen or transferred to foreign entities, this may provide them with extensive information about the subject» [14]. As a result of the public discussions surrounding the dactyloscopic registration of citizens of the Republic of Kazakhstan, a legal norm was adopted establishing that citizens have the right to undergo fingerprint registration and (or) provide biological material only upon their consent.

One of the key challenges lies in the inability of the state to exercise direct control over the information systems of private companies. Previously, the Ministry of Digital Development, Innovations, and Aerospace Industry of the Republic of Kazakhstan emphasized the need to strengthen oversight of private-sector databases. This issue arises from the absence of a unified centralized data management system in the country.

Domestic scholars believe that this issue can be addressed through the introduction of a supervisory mechanism and continuous monitoring using information and communication technologies, including blockchain technology. Such technologies exclude the possibility of unauthorized access to personal data. «To minimize the risks of data leakage and unauthorized processing of personal information, it is recommended that all records be maintained through a blockchain-based architecture. This decentralized structure provides a higher degree of data integrity and protection against external interference. The key benefit of blockchain lies in its ability to preserve the confidentiality and authenticity of stored information, effectively eliminating the possibility of unauthorized disclosure or modification without the explicit consent of the data owner» [15].

Blockchain is a distributed database (ledger) organized as a chain of interconnected blocks used for storing data. Each block contains information about transactions and is linked to the previous through cryptographic encryption.

Blockchain technology is characterized by the following key features:

1) Decentralization – the system operates without a central governing authority, while data is stored simultaneously across multiple nodes within the system;

2) Immutability of data – once information is recorded in a block and confirmed, it cannot be altered, which ensures protection against fraud and data falsification;

3) Transparency – all participants in the system have access to the transaction history.

4) Cryptographic security – blocks are linked using cryptographic hash functions, while each transaction is verified and confirmed by an electronic digital signature, ensuring its authenticity.

5) Consensus mechanisms – the addition of a new block requires agreement among network participants in accordance with a specific algorithm, such as Proof of Work, Proof of Stake and others;

6) Smart contracts – blockchain technology enables the creation of programmable algorithms, known as smart contracts, which are executed automatically once predefined conditions are met.

7) Reliability and resilience – even if one node fails or is compression, the data remains preserved on other nodes within the network. [16].

The socio-economic effectiveness of work blockchain technology lies in its ability to eliminate intermediary barriers, reduce transaction costs, enhance the reliability and accessibility of data, and strengthen trust among participants in economic and public governance relations.

Unfortunately, most citizens lack basic knowledge of personal data protection rules. The requirements governing the use of electronic digital signatures are frequently violated, which, in our view, is attributable to the low level of digital literacy within society.

As an information security expert observes, even after submitting a loan application, citizens do not always fully understand their rights. According to experts, if an individual refuses to obtain a loan or open a bank account, they have the full legal right to submit a written request to the bank for the deletion of previously provided personal data. However, the majority of citizens do not exercise this right and are often unaware of its existence [17].

At present, the Parliament of the Republic of Kazakhstan has commenced discussions on the draft Digital Code. In the latest version of the draft, dated 3 September 2025, the concept of «digital data» is introduced, along with the definition of their identifiers. Paragraph 3 of Article 22 provides that: «Unique public identifiers shall constitute publicly available data processed in accordance with this Code, taking into account the legislation of the Republic of Kazakhstan on personal data and their protection» [18]. However, this provision contradicts paragraph 2-1 of Article 7 of the Law of the Republic of Kazakhstan «On Informatization». Pursuant to this provision, Order No. 526/NK of the Minister of Digital Development, Innovations, and Aerospace Industry of the Republic of Kazakhstan dated 29 August 2024 approved the «List of Personal Data of Individuals Included in the Composition of State Electronic Information Resources». This order recognizes the Individual Identification Number (IIN) as personal data included in the structure of state electronic resources. According to the current legislation and the draft Digital Code, such data may be used only with the consent of the data subject or their legal representative. Therefore, it is proposed to delete the words «publicly available data» from the text of the draft as inconsistent with the law.

Paragraph 3 of Article 24 of the draft Digital Code, which regulates biometric identification, provides the following: «For the purposes of identification, the following biometric data of citizens of the Republic of Kazakhstan shall be subject to processing:

1. «digital facial image»;

2. «dactyloscopic information» [18].

According to subparagraph 38-1 of paragraph 1 of Article 1 of the Law of the Republic of Kazakhstan «On Informatization» (No. 418-V, 24 November 2015), «biometric identification is a set of measures aimed at establishing a person's identity on the basis of their immutable physiological and biological characteristics» [19].

Furthermore, paragraph 1 of Article 1 of the Law of the Republic of Kazakhstan «On Personal Data and Their Protection» defines «biometric data as personal data characterizing the physiological and biological features of a personal data subject, on the basis of which such a person may be identified».

Thus, the current legislation does not provide a comprehensive and detailed definition of the concept of biometric data. This is due to the fact that, as mentioned above, the category of biometric data should include not only fingerprint information, but also DNA analysis results, distinctive facial features and expressions, the iris of the eye, as well as other physiological and biological characteristics that make it possible to identify a person or associate specific data

with an individual. Such characteristics include a person's facial image (in the form of a photo and video recordings).

In the global biometric systems market, the following technologies based on biometric recognition are actively utilized:

1. Fingerprints – over 50% of the market;
2. Facial recognition – 21,6%;
3. Iris recognition – 10,2%;
4. Voice recognition – 4%;
5. Retinal pattern recognition – 3%;
6. Palm geometry, DNA, and other identifiers – approximately 7%.

Therefore, the draft Digital Code does not provide for an exhaustive list of biometric data to be registered as biometric data of citizens to be processed for identification purposes included in paragraph 3 of Article 24. For example, we concluded that genomic information (DNA), the retinal pattern, iris image and voice data should also be included.

It should also be noted that Kazakhstan has not ratified international instruments on the protection of personal data, in particular the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) (Strasbourg, 28 January 1981) [20].

An important direction for further development is the consideration of Kazakhstan's accession to this Convention. Such a step would grant the right to conduct investigations into violations of the personal data protection rights of Kazakhstani citizens by operators that are parties to the Convention. Moreover, the Convention establishes the right of every individual to be informed of the existence of automated databases containing their personal information, their main purposes, as well as the name and location of the data controller.

Although the above-mentioned convention has not been ratified by the Republic of Kazakhstan, the Law of the Republic of Kazakhstan «On Personal Data and Their Protection» dated May 21, 2013 (No. 94-V), which incorporates its key provisions, was adopted. At the legislative level, this represented an attempt to consolidate the fundamental rules governing the processing and protection of citizens' personal data within a single legal act. However, according to many experts in this field, the adoption of the Law of the Republic of Kazakhstan «On Personal Data and Their Protection» resulted in only short-term positive effects.

A major turning point in the development of personal data protection mechanisms was the adoption of the General Data Protection Regulation (GDPR) by the European Union in 2016. This instrument laid the foundation for the modernization and legal consolidation of personal data protection systems in developed countries [20].

The GDPR brought about profound changes in the regulation of personal data processing across the EU. It significantly transformed existing approaches to data handling, increased awareness of personal data protection issues among both professionals and the public, and expanded the rights of individuals to control the use of their personal data. As a result, EU citizens became better informed and more autonomous in exercising their data protection rights. These developments were confirmed by the results of a survey conducted among EU citizens within the framework of the Eurobarometer project in 2019 [21].

In addition to introducing stricter regulatory requirements, the GDPR granted EU citizens a number of new rights, including the right to request the erasure of personal data, thereby considerably strengthening individual control over personal information. Comparable legal mechanisms are largely absent from the current legislation of the Republic of Kazakhstan.

A comparison of the Law Republic of Kazakhstan «On Personal Data and Their Protection» with the legislation of foreign states shows that the Kazakhstani law is relatively detailed and comprehensive in its formulation. Nevertheless, practical implementation reveals a number of significant shortcomings in ensuring personal data security. In particular, the law does not provide a clear concept of «personal data processing». Moreover, Article 2 of the Law does not explicitly cover activities related to the storage of personal data. As a result, violations affecting the integrity, confidentiality and availability of citizens' personal data are not clearly delineated in legislation. This regulation gap has led to risks and threats, including frequent cases of loss of personal data in both electronic and paper form, which has resulted in a loss of control over data processing experienced among citizens.

Article 9 of the Law allows for the collection and processing of personal data without the consent of the data subject or their legal representative in certain cases. Among others, in practice, such situations arise during elections and referendums. However, neither the Law Republic of Kazakhstan «On Personal Data and Their Protection» nor the Constitutional Law of the Republic of Kazakhstan «On Elections» establishes clear procedures for the collection, processing and storage of personal data during electoral processes at any level.

Clause 2 of Article 25 of the Law imposes an obligation on the owner or operator to take measures to destroy personal data once the purposes of its collection and processing have been achieved. At the same time, the legislation does not regulate mechanisms of ongoing control and monitoring by the owner and/or operator, nor does it define the responsibilities of persons organizing the collection and processing of personal data. This legal uncertainty created conditions under which responsible parties may avoid liability in cases of incomplete destruction or loss of personal data. From this perspective, it is necessary to develop technological solutions that prevent unauthorized access to personal data, while simultaneously imposing clear legal obligations on responsible persons or operators to ensure continuous control and monitoring of the data destruction process.

Current legislation also fails to regulate personal data storage as an independent stage of data processing, including requirements related to data integrity, confidentiality and availability. The absence of such regulation significantly increases the vulnerability of stored data and facilitates breaches of data security. Comprehensive regulation of personal data storage prior to the introduction of blockchain technology as a data protection mechanism would significantly reduce these risks.

In recent years, blockchain technology has emerged as one of the most promoting tools in the field of information security for the collection, processing, storage and transfer of personal data. While many states are actively developing personal data, the Republic of Kazakhstan still lacks a coherent conceptual approach to ensuring data security throughout the entire lifecycle of personal data. For this reason, before implementing blockchain based solutions, it is necessary to adopt «National Regulation on the Protection of Personal Data based on Blockchain Technology». Such regulation would ensure transparency in data processes and provide for informed and reasonable consent of personal data subjects regarding the collection, processing, transfer and destruction of their data. Importantly, it would also grant citizens effective control over the movement and use of their personal data.

Conclusion

The Constitution of the Republic of Kazakhstan established legal guarantees for the exercise of the right to privacy and the inviolability of personal and family secrets. Therefore, all information concerning an individual's private and family life, financial situation, correspondence, or personal communications must remain confidential and may not be accessed or disclosed without the explicit consent of the data owner, except in instances clearly prescribed by law. Simultaneously, the Constitution of the Republic of Kazakhstan affirms every citizen's right to obtain access to documents, decisions, and materials that contain their personal data.

To ensure the realization of these constitutional guarantees, the Law «On Personal Data and Their Protection» defines personal data as information recorded in electronic or paper form, as well as on alternative media such as disks, flash drives, or other storage devices. However, the current legislation does not yet provide a clear definition of the legal status of personal information transmitted orally, which represents an unresolved issue within the national regulatory framework.

At present, in foreign countries, the security of personal data is ensured through the use of technologies such as blockchain, cryptography, distributed ledgers, and others. Applying this experience in our country, the processes of control and monitoring should be implemented through distributed ledger (blockchain) technologies, since, in our opinion, this approach helps prevent unauthorized access to personal data.

The improvement of national legislation can also be achieved by joining the international convention on the protection of personal data and by implementing its provisions into domestic law. For instance, within the European Union, the Directive (GDPR) establishes international standards for the protection of personal data. This would enhance the effectiveness of legal mechanisms for data protection, strengthen citizens' confidence in the security of their personal information, and provide a safeguard for the inviolability of private life.

In addition, the GDPR grants citizens of the European Union simple and accessible mechanisms to exercise their rights, while simplifying the procedure for submitting complaints to supervisory authorities.

At the present stage, the state faces an important task of ensuring the protection of personal data by strengthening control over digital threats and introducing a procedure for assessing their impact on human rights in accordance with international standards.

We believe that consideration of the above-mentioned mechanisms in the legislation will ensure the personal safety of citizens.

Authors' Contribution

The authors – **Tilep T.S., Juchnevicius E. –** made an equal contribution to the preparation of this article and the conduct of the research.

Tilep T.S. studied and substantiated the conceptual framework of the research, summarized and analyzed data from the literature and normative legal acts;

Juchnevicius E. examined the possibilities for adapting international norms in the field of personal data protection to the legislation of the Republic of Kazakhstan;

Both authors carried out the analysis and generalization of the research results and formulated the conclusions.

References

1. Қазақстан Республикасының 2029 жылға дейінгі ұлттық даму жоспарын бекіту және Қазақстан Республикасы Президентінің кейбір жарлықтарының күші жойылды деп тану туралы Қазақстан Республикасы Президентінің 2024 жылғы 30 шілдедегі №611 Жарлығы. –– Қолжетімділік тәртібі: https://adilet.zan.kz/kaz/docs/U2400000611 (дата обращения: 25.09.2025)

2. Продают за вознаграждение: в МВД рассказали о причинах утечки персональных данных. 12 сентября 2025 // https://www.zakon.kz/obshestvo/6490664-prodayut-za-voznagrazhdenie-v-mvd-rasskazali-o-prichinakh-utechki-personalnykh-dannykh.html (дата обращения: 25.09.2025)

3. Токаев поручил ужесточить ответственность за утечку персональных данных казахстанце // https://news.mail.ru/politics/67895150/ (дата обращения: 25.09.2025)

4. В сеть утекли данные более 16 миллионов казахстанцев. 17 июня 2025 года // Настоящее Время https://www.currenttime.tv/a/kazahstan-set-dannye/33446067.html (дата обращения: 25.09.2025)

5. President Kassym-Jomart Tokayev's State of the Nation Address to the People of Kazakhstan "Kazakhstan in the Era of Artificial Intelligence: Current Challenges and Solutions through Digital Transformation" // https://www.akorda.kz/en/president-kassym-jomart-tokayevs-state-of-the-nation-address-to-the-people-of-kazakhstan-kazakhstan-in-the-era-of-artificial-intelligence-current--challenges-and-solutions-through-digital-transformation-1083029 (дата обращения: 25.09.2025)

6. Глава государства провел совещание по вопросам развития искусственного интеллекта. 11 августа 2025 года // https://www.akorda.kz/ru/glava-gosudarstva-provel-soveshchanie-po-voprosam-razvitiya-iskusstvennogo-intellekta-1175749 (дата обращения: 25.09.2025)

7. Дербес деректер және оларды қорғау туралы Қазақстан Республикасының 2013 жылғы 21 мамырдағы №94-V Заңы. –– Қолжетімділік тәртібі: https://adilet.zan.kz/kaz/docs/Z1300000094#z21 (дата обращения: 25.09.2025)

8. Директива Европейского Парламента и Совета Европейского Союза от 12 июля 2002 года № 2002/58/ЕС «В отношении обработки персональных данных и защиты конфиденциальности в секторе электронных средств связи» (Директива о конфиденциальности и электронных средствах связи) (в редакции Директивы 2006/24/ЕС Европейского парламента и Совета ЕС от 15 марта 2006 г., Директивы 2009/136/ЕС Европейского парламента и Совета ЕС от 25 ноября 2009 г.). – Режим доступа: https://online.zakon.kz/Document/?doc_id=31067636 (дата обращения: 25.09.2025)

9. Соколова О.С. Персональные данные как информация ограниченного доступа: проблемы правового регулирования // Современное право. – 2004. – №2. – С.18-21.; 19

10. Мемлекеттік құпиялар туралы Қазақстан Республикасының 1999 жылғы 15 наурыздағы №349-I Заңы. – – Қолжетімділік тәртібі: https://adilet.zan.kz/kaz/docs/Z990000349_ (дата обращения: 25.09.2025)

11. Дербес деректер және оларды қорғау туралы Қазақстан Республикасының 2013 жылғы 21 мамырдағы №94-V Заңы. – Қолжетімділік тәртібі: https://adilet.zan.kz/kaz/docs/Z1300000094#z21 (дата обращения: 25.09.2025)

12. Турысбекулы М. Без лица?! Изображение лица, как персональные данные. – Режим доступа: https://online.zakon.kz/Document/?doc_id=35173317&pos=6;-106#pos=6;-106 (дата обращения: 25.09.2025)

13. Иксанова Н. Всеобщий сбор отпечатков пальцев: можно ли верить государству? Мнение экспертов.– Режим доступа: https://bes.media/news/vseobschij-sbor-otpechatkov-palcev-mozhno-li-verit-gosudarstvu-mnenie-ekspertov-2626/ (дата обращения: 25.09.2025)

14. Айдарбек Н. «Биометрию можно подделать»: новая лазейка для мошенников появится в Казахстане? – Режим доступа: https://golos-naroda.kz/21195-biometriiu-mozhno-poddelat-novaia-lazeika-dlia-moshennikov-poiavitsia-v-kazakhstane-1697198372/ (дата обращения: 25.09.2025)

15. Ilyassova, G., Aitimov, B., Zhumagulov, M & Zhamburbayeva, S. (2025). Ensuring Personal Data Security Using Blockchain Technology: Issues and Perspectives for Legislative Improvement. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction в Volume 18, Issue 1 // https://ascelibrary.org/doi/10.1061/JLADAH.LADR-1248 DOI: https://doi.org/10.1061/JLADAH.LADR-1248 (дата обращения: 25.09.2025)

16. Ильясова Г.А., Сабыржан А., Айтимов Б.Ж., Токатов Р.А., Жамбурбаева С. Қазақстан Республикасында блокчейн технологиясын қолдануды құқықтық реттеудің теориялық және тәжірибелік мәселелері. Монография. / Ред. Г.А. Ильясова. – Қарағанды: Colorprint ЖШС баспасы, 2025. – 336 бет.

17. Киберугроза: почему произошла утечка персональных данных Пятница, 01 Авг 2025. КАЗИНФОРМ//https://ratel.kz/raw/kiberugroza_pochemu_proizoshla_utechka_personalnyh_dannyh (дата обращения: 25.09.2025)

18. Досье на проект Цифрового кодекса Республики Казахстан (сентябрь 2025 года) // https://online.zakon.kz/Document/?doc_id=38933548 (дата обращения: 25.09.2025)

19. Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января, 1981 г.) (с изменениями от 15 июня 1999 г.) – Режим доступа: https://online.zakon.kz/Document/?doc_id=1034061&pos=1;-12#pos=1;-12 (дата обращения: 25.09.2025)

20. Регламент № 2016/679 Европейского парламента и Совета Европейского Союза О защите физических лиц при обработке персональных данных и о свободном обращении таких данных, а также об отмене Директивы 95/46/ЕС. – Режим доступа: https://online.zakon.kz/Document/?doc_id=39559334&pos=5;-106#pos=5;-106

21. Malia Thuret-Benoist, “One year of GDPR: GDPR enforcement and awareness,” Tech GDPR, May 25, 2019. –– Access mode: https://techgdpr.com/blog/one-year-gdpr/

Т.С. Тілеп[1], Э.Юхневичус[2]

[1]Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зерттеу университеті, Қарағанды, Қазақстан

[2]Гданьск университеті, Гданьск, Польша

(e-mail: tlep97@mail.ru[1], e.juchnevicius@prawo.ug.edu.pl[2])

Қазақстан Республикасында азаматтардың дербес деректерін қорғаудың құқықтық мәселелері

Аңдатпа: Мақалада жеке деректерді қорғау туралы заңнаманың бүгінгі жай-күйі, оны іске асыру барысында туындаған мәселелер және блокчейн технологиясын қолдану арқылы қорғау тетігін жетілдірудің перспективалары қарастырылған. Қазақстанда дербес деректердің заңсыз таралу жағдайларының жиі орын алуы киберқауіпсіздік мәселесінің шешілмеуіне тікелей байланысты болуы, қолданыстағы заңнаманың осал тұстарын жетілдіру қажеттігі зерттеу тақырыбының өзектілігін айқындап береді. Зерттеу мақсаты – цифрлық технологияларды қолдану арқылы дербес деректердің қорғалуын, қауіпсіздігін қамтамасыз етуге қол жеткізетін құқықтық негіздерді қалыптастыру. Жұмыстың ғылыми жаңалығы Қазақстан Республикасында

дербес деректер институтын реттейтін заңнамалық кешен қалыптасқаннан кейін алғаш рет дербес деректердің құқықтық табиғатын, дербес деректердің жекелеген түрлерінің айналымын құқықтық реттеу бағыттарын анықтауы, дербес деректердің айналымын реттейтін қолданыстағы заңнаманы жетілдіруге бағытталған ұсыныстарды беруі болып табылады. Олар дербес деректерді қорғау саласында ұлттық ғылыми доктринаны қалыптастырады. Тәжірибелік маңызы жаңа тәжірибелік маңызды тұжырымдар қортындыланады, олар қолданыстағы ұлттық заңнаманы жетілдіруге мүмкіндік береді. Сондықтан, оларды құқық шығармашылық саласында қолдануға болады. Зерттеу тәсілдері ретінде жалпы логикалық тәсілдер (индукция, дедукция), жүйелендіру, талдау, тұжырымдау, ғылыми тәсілдер, эмпирикалық тәсілдер қолданылды.

Дербес деректердің қауіпсіздігін қамтамасыз ету – мемлекеттің адамның жеке құқықтарын қорғау міндеті болғандықтан, авторлар цифрлық қауіптерді бақылауды күшейту, халықаралық стандарттарға сәйкес адам құқықтарына әсерді бағалау рәсімін енгізу қазіргі кезеңде өте маңызды деп атап көрсетіледі. Ол үшін дербес деректерді қорғау стандарттарын орнататын халықаралық актілерге Қазақстан Республикасының қосылуы қажет деген қорытынды жасалады. Дербес деректерді қорғау саласындағы заңдарды жетілдірудің бір жолы – дербес деректерге заңсыз қол жеткізу мүмкіндігін болдырмайтын тетіктер енгізу және оны деректердің бақылаушысы (иесі, оператор) секілді тараптарды да қамтитын деңгейде іске асыру маңызды. Зерттеу нәтижесінде, қолданыстағы заң бойынша меншік иесі және оператор, сондай-ақ дербес деректерді өңдеуді және сақтауды ұйымдастыруға жауапты тұлға тарапынан тұрақты бақылау және мониторинг процесін реттейтін норма қабылдау қажеттігі жөнінде пікір білдірілген.

Түйін сөздер: цифрландыру, Цифрлық кодекс, дербес деректер, биометриялық деректер, сәйкестендіру, дербес деректерді қорғау, киберқауіпсіздік.

Т.С. Тілеп[1], Э.Юхневичус[2]

[1]Карагандинский национальный исследовательский университет имени академика Е.А. Букетова, Караганды, Казахстан

[2]Гданьский университет, Гданьск, Польша

(e-mail: tlep97@mail.ru[1], e.juchnevicius@prawo.ug.edu.pl[2])

Правовые проблемы защиты персональных данных граждан в Республике Казахстан

Аннотация: В статье рассматриваются современное состояние законодательства о защите персональных данных, возникающие проблемы при его реализации, а также перспективы совершенствования механизма защиты с использованием технологии блокчейн. Частые случаи незаконного распространения персональных данных в Казахстане напрямую связаны с нерешённостью вопросов кибербезопасности, что подчёркивает актуальность темы исследования и необходимость совершенствования уязвимых положений действующего законодательства. Цель исследования заключается в формировании правовой основы, обеспечивающей защиту и безопасность персональных данных посредством использования цифровых технологий. Научная новизна работы заключается в том, что впервые с момента формирования законодательного комплекса, регулирующего институт персональных данных в Республике Казахстан, определены правовые нормы в отношении персональных данных, а также направления правового регулирования оборота отдельных видов персональных данных и предложены меры по совершенствованию существующего законодательства, регулирующего

оборот персональных данных. Изложенное образует общенациональную научную доктрину в области защиты персональных данных. Обобщены новые практические выводы, позволяющие усовершенствовать существующее национальное законодательство и, следовательно, применять их в законотворческой деятельности. В качестве методов исследования использованы общелогический подход (индукция, дедукция), систематизация, анализ, формулировка, научные методы и эмпирические методы.

Обеспечение безопасности персональных данных является обязанностью государства по защите личных прав человека, поэтому авторы подчёркивают важность усиления контроля над цифровыми угрозами, а также введения процедуры оценки воздействия на права человека в соответствии с международными стандартами. Делается вывод о необходимости присоединения Республики Казахстан к международным актам, устанавливающим стандарты защиты персональных данных. Один из путей совершенствования законодательства в сфере защиты персональных данных — внедрение механизмов, исключающих возможность незаконного доступа к данным, и реализация этих механизмов на уровне, охватывающем такие стороны, как контролёр данных (владелец, оператор). По результатам исследования высказано мнение о необходимости принятия нормы, регулирующей процесс постоянного контроля и мониторинга со стороны владельца, оператора, а также ответственного лица за организацию обработки и хранения персональных данных в соответствии с действующим законодательством.

Ключевые слова: Цифровизация, Цифровой кодекс, персональные данные, биометрические данные, идентификация, защита персональных данных, кибербезопасность.

References

1. Qazaqstan Respublikasynyn 2029 jylga deiıngı ulttyq damu josparyn bekıtu jane Qazaqstan Respublikasy Prezidentının keibır jarlyqtarynyn kusı joiyldy dep tanu turaly Qazaqstan Respublikasy Prezidentının 2024 jylgy 30 sıldedegı №611 Jarlygy. – Qoljetımdılık tartıbı: https://adilet.zan.kz/kaz/docs/U2400000611 (data obrasenia: 25.09.2025) [in Kazakh]

2. Prodaiut za voznagrajdenie: v MVD rasskazali o prichinah utechki personalnyh dannyh. 12 sentabra 2025 // Dostupno po adresu: https://www.zakon.kz/obshestvo/6490664-prodayut-za-voznagrazhdenie-v-mvd-rasskazali-o-prichinakh-utechki-personalnykh-dannykh.html (data obrasenia: 25.09.2025) [in Russian]

3. Tokaev poruchil ujestochit otvetstvennost za utechku personalnyh dannyh kazahstanse // Dostupno po adresu: https://news.mail.ru/politics/67895150/ (data obrasenia: 25.09.2025) [in Russian]

4. V set utekli dannye bolee 16 millionov kazahstansev. 17 iuna 2025 goda // Nastoiasee Vrema Dostupno po adresu: https://www.currenttime.tv/a/kazahstan-set-dannye/33446067.html (data obrasenia: 25.09.2025) [in Russian]

5. President Kassym-Jomart Tokayev's State of the Nation Address to the People of Kazakhstan "Kazakhstan in the Era of Artificial Intelligence: Current Challenges and Solutions through Digital Transformation" // Available at: https://www.akorda.kz/en/president-kassym-jomart-tokayevs-state-of-the-nation-address-to-the-people-of-kazakhstan-kazakhstan-in-the-era-of-artificial-intelligence-current-challenges-and-solutions-through-digital-transformation-1083029 (accessed: 25.09.2025)

6. Glava gosudarstva provel sovesanie po voprosam razvitia iskusstvennogo intellekta. 11 avgusta 2025 goda // Dostupno po adresu: https://www.akorda.kz/ru/glava-gosudarstva-provel-soveshchanie-po-voprosam-razvitiya-iskusstvennogo-intellekta-1175749 (data obrasenia: 25.09.2025) [in Russian]

7. Derbes derekter jane olardy qorgau turaly Qazaqstan Respublikasynyn 2013 jylgy 21 mamyrdagy №94-V Zany. – Qoljetımdılık tartıbı: https://adilet.zan.kz/kaz/docs/Z1300000094#z21 (data obrasenia: 25.09.2025) [in Kazakh]

8. Direktiva Evropeiskogo Parlamenta i Soveta Evropeiskogo Soiuza ot 12 iula 2002 goda № 2002/58/ES «V otnosenii obrabotki personalnyh dannyh i zasity konfidensialnosti v sektore elektronnyh sredstv svazi» (Direktiva o konfidensialnosti i elektronnyh sredstvah svazi) (v redaksii Direktivy 2006/24/ES Evropeiskogo parlamenta i Soveta ES ot 15 marta 2006 g., Direktivy 2009/136/ES Evropeiskogo parlamenta i Soveta ES ot 25 noiabra 2009 g.). – Dostupno po adresu: https://online.zakon.kz/Document/?doc_id=31067636 (data obrasenia: 25.09.2025) [in Russian]

9. Sokolova O.S. (2004) Personalnye dannye kak informasia ogranichennogo dostupa: problemy pravovogo regulirovania // Sovremennoe pravo. – №2. – S.18-21.; 19 [in Russian]

10. Memlekettık qupialar turaly Qazaqstan Respublikasynyn 1999 jylgy 15 nauryzdagy №349-I Zany. – Qoljetımdılık tartıbı: https://adilet.zan.kz/kaz/docs/Z990000349_ (data obrasenia: 25.09.2025) [in Kazakh]

11. Derbes derekter jane olardy qorgau turaly Qazaqstan Respublikasynyn 2013 jylgy 21 mamyrdagy №94-V Zany. – Qoljetımdılık tartıbı: https://adilet.zan.kz/kaz/docs/Z1300000094#z21 (data obrasenia: 25.09.2025) [in Kazakh]

12. Turysbekuly M. Bez lisa?! Izobrajenie lisa, kak personalnye dannye. – [Elektronnyi resurs]. – Dostupno po adresu: https://online.zakon.kz/Document/?doc_id=35173317&pos=6;-106#pos=6;-106 (data obrasenia: 25.09.2025) [in Russian]

13. İksanova N. Vseobsi sbor otpechatkov palsev: mojno li verit gosudarstvu? Mnenie ekspertov.– Dostupno po adresu: https://bes.media/news/vseobschij-sbor-otpechatkov-palcev-mozhno-li-verit-gosudarstvu-mnenie-ekspertov-2626/ (data obrasenia: 25.09.2025) [in Russian]

14. Aidarbek N. «Biometriu mojno poddelat»: novaia lazeika dla mosennikov poiavitsa v Kazahstane? – Dostupno po adresu: https://golos-naroda.kz/21195-biometriiu-mozhno-poddelat-novaia-lazeika-dlia-moshennikov-poiavitsia-v-kazakhstane-1697198372/ (data obrasenia: 25.09.2025) [in Russian]

15. Ilyassova, G., Aitimov, B., Zhumagulov, M & Zhamburbayeva, S. (2025). Ensuring Personal Data Security Using Blockchain Technology: Issues and Perspectives for Legislative Improvement. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction в Volume 18, Issue 1 // Available at: https://ascelibrary.org/doi/10.1061/JLADAH.LADR-1248%20%20DOI:%20https://doi.org/10.1061/JLADAH.LADR-1248 (Date of access: 25.09.2025)

16. Ilasova G.A., Sabyrjan A., Aitimov B.J., Tokatov R.A., Jamburbaeva S. Qazaqstan Respublikasynda blokchein tehnologiasyn qoldanudy quqyqtyq retteudın teorialyq jane tajıribelık maseleleri. Monografia. / Red. G.A. Ilasova. – Qaragandy: Colorprint JŞS baspasy, 2025. — 336 bet. [in Kazakh]

17. Kiberugroza: pochemu proizosla utechka personalnyh dannyh Patnisa, 01 Avg 2025. KAZİNFORM // https://ratel.kz/raw/kiberugroza_pochemu_proizoshla_utechka_personalnyh_dannyh (data obrasenia: 25.09.2025) [in Russian]

18. Döse na proekt Sifrovogo kodeksa Respubliki Kazahstan (sentabr 2025 goda) // Dostupno po adresu: https://online.zakon.kz/Document/?doc_id=38933548 (data obrasenia: 25.09.2025) [in Russian]

19. Konvensia o zasite fizicheskih lis pri avtomatizirovannoi obrabotke personalnyh dannyh (Strasburg, 28 ianvara, 1981 g.) (s izmeneniami ot 15 iuna 1999 g.) // Dostupno po adresu: https://online.zakon.kz/Document/?doc_id=1034061&pos=1;-12#pos=1;-12 (data obrasenia: 25.09.2025) [in Russian]

20. Reglament № 2016/679 Evropeiskogo parlamenta i Soveta Evropeiskogo Soiuza O zasite fizicheskih lis pri obrabotke personalnyh dannyh i o svobodnom obrasenii takih dannyh, a takje ob otmene

Direktivy 95/46/ES. – Rejim dostupa: https://online.zakon.kz/Document/?doc_id=39559334&pos=5;-106#pos=5;-106 [in Russian]

21. Malia Thuret-Benoist, "One year of GDPR: GDPR enforcement and awareness," Tech GDPR, May 25, 2019. – Access mode: https://techgdpr.com/blog/one-year-gdpr/

Information about the authors:

Tilep T. **–** corresponding author, Master of Juridical Sciences, PhD student, Department of Civil and Labor Law, Buketov Karaganda National Research University, 28 Universitetskaya st., 100028, Karaganda, Kazakhstan

Juchnevicius E. **–** Doctor hab., International Cooperation Coordinator, Faculty of Law and Administration, University of Gdańsk, 6 Jana Bażyńskiego st.,80-309, Gdańsk, Poland

Тілеп Т.С. **–** хат-хабар авторы, заң ғылымдарының магистрі, Академик Е.А. Бөкетов атындағы Қарағанды ұлттық зертту университетінің Азаматтық және еңбек құқығы кафедрасының докторанты, Университетская көшесі, 28, 100028, Қарағанды, Қазақстан

Юхневичус Э. **–** PhD докторы, dr hab., Құқық және әкімшілік факультетінің профессоры, Гданьск университеті, Jana Bażyńskiego көшесі, 6., 80-309, Гданьск, Польша

Тілеп Т.С. – автор для корреспонденции, магистр юридических наук, докторант кафедры гражданского и трудового права Карагандинского национального исследовательского университета имени академика Е.А. Букетова, ул.Университетская, 28, 100028, Караганда, Казахстан.

Юхневичус Э. – Доктор PhD, dr hab., профессор факультета права и администрации, Гданьский университет, ул. Jana Bażyńskiego, 6., 80-309, Гданьск, Польша.