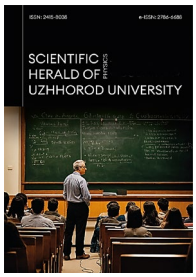
Scientific Herald of Uzhhorod University
Series "Physics"
Journal homepage: https://physics.uz.ua/en
Issue 55, 2174–2186
Received: 21.12.2023. Revised: 11.02.2024. Accepted: 28.03.2024



DOI: 10.54919/physics/55.2024.217wl4

Legal ways and methods of personal data protection in Kazakhstan

Almas Amirov*
Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan
010078, 94 Republic Str., Kosshy, Republic of Kazakhstan

Dariga Kainazarova
Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan
010078, 94 Republic Str., Kosshy, Republic of Kazakhstan

Ernar Begaliyev
Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan
010078, 94 Republic Str., Kosshy, Republic of Kazakhstan

Azamat Sarsenbaev
Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan
010078, 94 Republic Str., Kosshy, Republic of Kazakhstan

Nurlybek Sarybayev
Law Enforcement Academy under the Prosecutor General's Office of the Republic of Kazakhstan
010078, 94 Republic Str., Kosshy, Republic of Kazakhstan

Abstract

Relevance. The relevance of the study lies in the need to develop theoretical ideas about this issue and identify promising areas for implementation in the legislation of the Republic of Kazakhstan, which today is not perfect in the context of legal regulation of personal data protection.

Purpose. The purpose of the study was to study the features of personal data protection in the Republic of Kazakhstan and other countries (European Union countries, the United States of America, and Brazil).

Methodology. The methodological basis of the article was the methods of statistical analysis, analogy and generalization, as well as comparative legal, formal legal and formal logical methods.

Results. The study revealed the features of the legal regulation of the protection of personal data under the legislation of the Republic of Kazakhstan. In addition, it was found that the legislation of the European Union contains additional obligations that are aimed at maximum protection of personal data. However, the current legislation of Kazakhstan is fragmented and does not fully pay due attention to the protection of personal data. In this regard, it was proposed to revise and update the rules for the protection of personal data for specific industries, taking into account their specifics. In addition, the importance of raising citizens' awareness of the rights and responsibilities in the field of the digital sphere is emphasized, which includes the popularization of knowledge about the safe use of the Internet, means of protecting personal data and cyber hygiene.

Suggested Citation:
Amirov A, Kainazarova D, Begaliyev E, Sarsenbaev A, Sarybayev N. Legal ways and methods of personal data protection in Kazakhstan. *Sci Herald Uzhhorod Univ Ser Phys.* 2024;(55):2174-2186. DOI: 10.54919/physics/55.2024.217wl4

*Corresponding author

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/

Conclusions. The role of active cooperation with international partners and organizations is noted, which will help to exchange experience and best practices in the field of digital security and personal data protection. Regular reviews and revisions of existing protection mechanisms, as well as the introduction of new technological solutions and innovations, will help ensure a sustainable and reliable digital ecosystem in the long term.

Keywords: information security; confidentiality; privacy; global Internet; experience of the European Union.

Introduction

In the era of intensive development of the big data sphere, there is a significant problem associated with the leakage of personal information. As part of the activities of the Ministry of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan, Order No. 395/NC of 2020, approving the rules for the collection and processing of personal data. This activity aims to improve the legal system that ensures the protection of personal data. However, despite the importance and significance of this normative act, its development was limited in time, which presents serious challenges for the effective legal protection of personal data in practice. According to the results of the study by A. Dzhaksylykov, 37% of respondents do not attach importance and do not see the need to ensure network security, justifying their position by the fact that in real life they already face a sufficient number of problems [1]. Moreover, according to the Center for Analysis and Investigation of Cyberattacks, the data leak occurred from the information system of the law enforcement agency of the Republic of Kazakhstan and affected information about all citizens of Kazakhstan and foreigners associated with administrative office work [2].

So, according to the provisions of the above-mentioned act, personal data of limited access can be included in information for official use. But today, in Kazakhstan there is no clear definition of what exactly belongs to this category of data, and this can cause practical difficulties [3]. Also, at the moment, the main risks are associated with the implementation of the relevant provisions. The question of how the personal data access control service will be implemented remains open, since information on the technical specification has not yet been published anywhere. In this regard, the study of this issue is of particular relevance.

In this context, it should be noted that the issue of ensuring the security of personal data attracts the attention of many scientists in Kazakhstan. For example, A.S. Akmalovich conducted a study of the international legal aspects of personal data protection regulation, especially in relation to information relating to a specific person or identifying a person [4]. As a result of the study, it is proposed to resolve a number of important aspects, namely: the definition of the scope and possible exceptions; determining the entities to which these provisions apply; establishing basic definitions such as “data”, “data subject”, “data user”; formulating basic principles; definition of cases of restriction of access rights; regulation of privacy and security issues; establishing the rights of data subjects; determining the data processing process and criteria for lawful processing; and the imposition of sanctions and the provision of administrative or judicial protection.

In the article by R. Akhambaev and Zh. Akhmetova considered the basic principles of ensuring the security of personal data of users in an organization [5]. In this article, special attention is paid to recommendations for the protection of personal data, which are the assets of the organization. Based on the research, it emphasizes the importance of optimizing the scale of threats, even without the need for auditing and applying risk management methods. The research of B. Maksutov is devoted to the creation of an authorized body for the protection of personal data in the Republic of Kazakhstan [6]. This study presents the legal structure of such a body, its mission, goals, objectives, and principles of activity. Practical recommendations are also presented, based on the world and case practice of the European Court of Human Rights (ECHR), regarding the establishment of a body for the protection of personal data. The author of the study proposes to introduce a separate legal mechanism to ensure the right to protection of personal data by creating a Personal Data Protection Authority.

F.M. Syrlybaeva conducted a study, during which the provisions on the protection of information rights of employees in Kazakhstan and in some foreign countries were considered [7]. As a result of the study, gaps in the legal regulation of the protection of information rights were identified, and certain conclusions were drawn in the field of protecting the labour information of employees. The article by M.S. Bissaliyev and K.N. Shakirov explored the main approaches to using knowledge of digital footprints on the Internet as an important factor in ensuring the safe handling of personal data in a cyber-environment [8]. The article presents the author’s definition of digital traces and proposes an algorithm for identifying ways to violate the security of personal data using a global information network. Typical phases of such violations and common actions of offenders are also shown. As a result of the study, proposals were made to adopt an international or regional (European) act that would set standards for the use of specialized knowledge in detecting illegal access to personal data, including their interception as part of information exchange on the Internet.

Nevertheless, it is worth noting that in the legal literature of recent years, there are no comprehensive fundamental studies related to the chosen topic. In this regard, the purpose of this study is to describe modern methods and approaches to the protection of personal data in Kazakhstan, taking into account the experience of other countries: the countries of the European Union (EU), the USA, Brazil and the practice of the ECHR, as well as the formation promising ways to improve the legislation of Kazakhstan in the field of personal data protection. The analogy method was used to compare the features of the legal regulation of personal data protection in different countries. The graphical method was used to visualize the results, and the logical generalization was used to systematize information about the state of the legislation of the Republic of Kazakhstan aimed at regulating the protection of personal data.

This study also used comparative legal, formal logical and formal legal methods, which made it possible to analyse the legal norms and provisions relating to the protection of personal data in different jurisdictions. To develop further approaches to the legal protection of personal data in the Republic of Kazakhstan, the method of logical generalization was used, which made it possible to systematize information and identify key aspects that require further study and improvement. Particular attention was paid to system analysis. It made it possible to consider the relationship and interaction of various elements and factors affecting the legal protection of personal data, which helped to better understand and assess the complexities and challenges faced by legal methods and approaches to the protection of personal data in Kazakhstan.

Theoretical and legal aspects of personal data protection: the experience of other countries

Protection of personal data is a set of measures that includes technical, organizational and organizational and technical measures aimed at ensuring the security of information related to a specific individual or allowing him to be identified. These measures also cover the protection of the rights, freedoms and fundamental interests of people in the context of the processing and use of their personal data, especially in conditions related to the use of information and communication technologies to simplify the process of information processing. The main purpose of such protection is to guarantee the use of personal data only in accordance with its intended purpose, as well as to provide data subjects with the right to correct possible errors.

It should be noted that the protection of personal data does not mean a complete restriction of access to this data. An important aspect is the organization of the correct procedure for obtaining and using personal information, which provides for informing data subjects about the purposes of using their personal data and providing access to information about the accumulated personal data. An important element of ensuring the human right to privacy is the confidentiality of information, which means ensuring the protection of access to personal data. In modern conditions of development of information and communication technologies, it is impossible to ensure complete anonymity. Various data such as information transmission time, amount of information, protocol, and format used may also be fixed. Therefore, when ensuring the protection and confidentiality of the transfer and receipt of personal information, it is necessary to take into account considerations about the expediency and necessity of ensuring public and state security.

Cross-border data transfer covers not only the personal data of individuals, but may also include a variety of data of an organizational, financial, technical, economic nature and other types of information. When studying various aspects of personal data protection, it should be noted that personal data can contain a wide range of information about a person, including financial, medical, identifying and other data. In this regard, there is a need for legal regulation of the protection of such data from illegal public distribution. Moreover, the concept of personal data protection may include not only the protection of information of individual individuals, but may also be relevant to legal entities. The dissemination and exchange of information can take place between international organizations or international companies providing services in the field of information transfer.

In the field of legal regulation of civil relations related to personal data, a system of regulatory standards has been developed, which is especially fully disclosed in the legal sources of the Council of Europe and the EU. In this context, it is important to note a number of international and European regulations aimed at protecting human rights and fundamental freedoms in the field of personal data processing. Such acts include the European Convention on Human Rights, adopted on November 4, 1950 [9], the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted on January 28, 1981 [10], the Directive of the European Parliament and of the Council No. 2002/58/EC "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data ", adopted on October 24, 1995 [11], as well as the Regulation of the European Parliament and of the council no. 2016/679 "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data" [12]. These documents establish general principles and standards for the protection of personal data in the EU. The study of these sources is due not only to their content, but also to the significant impact that they had on the convergence of civil law protection of the personal non-property sphere of individuals within the European legal space, at the level of the Council of Europe and the European Union.

With the advent of the Internet and the rapid growth of the exchange of information, including personal data, people began to knowingly or unconsciously provide their data for various purposes. However, given the global nature of the Internet and the free flow of data across borders, protecting the privacy and privacy of citizens has become critical. The EU first stepped in this direction with the adoption of the Data Protection Directive and later with the adoption of the General Data Protection Regulation (GDPR). The current GDPR regulation in the EU is bilateral: on the one hand, it grants rights and control over the data of subjects, and on the other hand, it restricts data processors in order to reduce the risks to the rights and freedoms of people related to the processing of personal data (Article 4(7) of the GDPR)) [12]. The GDPR is more sensitive to personal data than the US and China, providing additional protection. For example, the GDPR defines special categories of personal data such as genetic data and biometric data, along with other types of data such as race, trade union membership, sex life (Article 4(13) GDPR) [12]. The main principles for the protection of personal data under the GDPR are shown in Figure 1.

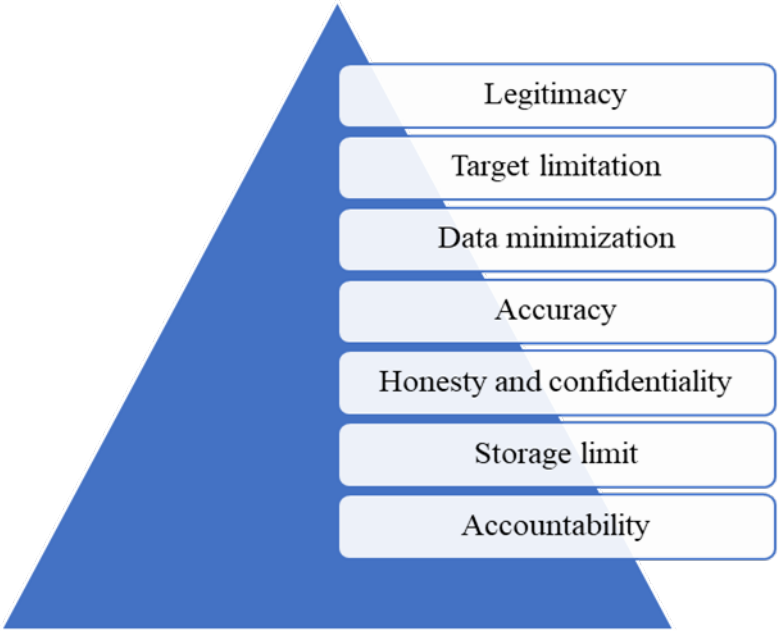


Figure 1. Basic principles of personal data protection under the GDPR

At the same time, other countries are usually more lenient, allowing companies and associations a greater degree of self-regulation, as, for example, in the case of the United States [14]. However, it should be noted that later the United States was forced to tighten some aspects of its regulation [16]. Thus, international and European law provides for significant preventive measures within the framework of regulatory relations to prevent violations of the rights of personal data subjects in the future. Due to the widespread collection and increasing threat to the security of personal data, some countries are enacting laws that give certain individuals control over the collection, processing, and transfer of personal data to public and private organizations. According to a 2018 Freedom House report, fifteen countries are considering data protection laws, and thirty-five countries already have such laws in place [17].

The adoption of legislative acts in various countries that establish the legal regime of information resources is the basis for the formation of a complex branch of law – information law. Its subject is public relations related to the legal regulation of the circulation of information, its creation, storage, processing, and use based on communication technologies, as well as its protection. The need to protect personal data arises in connection with the rapid development of informatisation, including the development of information and communication technologies, and the emergence of modern threats that can violate privacy. States that do not have an appropriate regulatory framework face problems in the field of personal data protection on the Internet, as well as restrictions on the transfer of such data due to the actions of foreign states. This may have a negative impact on the development of foreign economic activity.

Practice of the ECHR

The practice of the ECHR has developed criteria for the legitimate restriction of rights to personal data, which are consistent with the general principles of legitimate interference with private life. These criteria include the following: the interference must be in accordance with the law, have a legitimate aim and be necessary in a democratic society. The principle of the legality of the processing of personal data is further clarified through the practice of the ECHR. In this practice, the concept of "according to the law" is interpreted not only as a requirement that the relevant measures have a certain basis in law, but also as a requirement for the quality of this law.

This means that the law must be accessible to persons concerned with personal data and must predictably affect the consequences of its application. Accessibility of the law implies that the normative legal act must be promulgated. Predictability means that the norm must be clear so that the person can, if necessary, regulate his behaviour with the help of appropriate support [18].

The legitimacy of the goal pursued will be determined if it is consistent with the public interest listed in Article 8(2) of the Convention or the rights and freedoms of others. An interference will be necessary in a democratic society if it meets a pressing social need and is proportionate to the legitimate aim pursued. For example, when checking a candidate for an important position that is significant from the point of view of national security, the interests of national security may prevail over the private interests of the subject of personal data [19]. Thus, the practice of the ECHR defines the criteria and restrictions that must be observed for the lawful processing of personal data and the protection of the rights and freedoms of citizens. The concept of "personal data", according to the ECHR, includes not only information about "private life", which should not be interpreted narrowly, since respect for private life includes the right to establish and develop relationships with other people, as well as information about professional and business activities [18]. In addition, public information can be considered "private life" if it is systematically collected and stored in databases owned by public authorities [20].

The ECHR has considered a wide range of personal data, covering the following examples: data collected in official population censuses, including information on gender, marital status, place of birth, ethnicity, and other personal information; the taking of fingerprints, photographs, cell samples, DNA profiles and other personal or public information by the police, even if conditions of confidentiality are observed; collection and storage of medical data and other medical records; the requirement to provide detailed information on personal expenses for tax purposes (disclosure of intimate aspects of private life); listening, recording and storing telephone conversations; personal identification systems developed for administrative and civil purposes, such as databases in the field of health care, social assistance and tax authorities; video recordings made by video surveillance systems on the street; systems for intercepting conversations between prisoners and their relatives in visiting rooms in penitentiary institutions. Thus, the ECHR establishes a wide range of personal data to which its decisions apply, and examples that illustrate the variety of situations in which personal data is processed. This helps to define the boundaries and protection of data subjects' rights under national law. Among the rights of the subject of personal data identified in the practice of the ECHR, the following can be noted:

1. The right to access their personal data, which includes the negative duty of the state not to arbitrarily interfere in private life, limiting the ability of a person to access information about himself that is collected, stored, used and transmitted by state bodies. This right stems from the positive duty of the State to ensure respect for private life by establishing mechanisms for access to personal data. The right of access must be effective, that is, not only provide the opportunity to familiarize oneself with personal data and draw up one's own written extracts, but also provide the opportunity to receive copies of documents with personal data. In addition, this right must be exercised within a reasonable time. Restrictions on the right to access personal data may be established in the interests of the state, for example, to protect national security, as well as in private interests, for example, to protect the confidential information of third parties.
2. Ensuring the protection of personal data implies a positive duty of the state to ensure respect for private life by introducing a system of rules and guarantees aimed at protecting data. This includes a practical and effective security mechanism that prevents unauthorized access to personal data.
3. The right to change or destroy one's personal data is one of the rights recognized by the ECHR. According to judicial practice, the refusal to provide an opportunity to refute incorrect personal data is a violation of the right to respect for private life guaranteed by Article 8 of the Convention [19]. In addition, the positive duty of the state to ensure respect for private life includes the establishment of procedures that allow changes to be made to personal data, including information on ethnic origin. The ECHR also recognizes the so-called right to be forgotten, which provides that prolonged storage of personal data without sufficient justification may constitute a disproportionate interference with the right to respect for private life.

The ECHR, upon detection of a violation of the European Convention on Human Rights, may apply various measures to protect the rights of the subject of personal data. Some of these measures are listed below:

1. Awarding fair satisfaction to the injured party, which includes compensation for both moral and property damage. Compensation for non-pecuniary damage may be expressed in monetary terms, or it may be recognized that the mere recognition of a violation of the Convention and its consequences is a sufficient form of fair satisfaction.
2. Restoration of the previous legal status, as far as possible, that the personal data subject had before the violation of the Convention.
3. Application of other measures provided for in the decision of the ECHR, which may be aimed at ensuring effective protection of the rights of the subject of personal data.

So, the practice of the ECHR has formulated criteria that determine the lawful restriction of rights to personal data, in accordance with the general principles of lawful interference with private life. According to these criteria, the interference must comply with the law. This means that measures taken to limit the rights to personal data must have a legal basis and be provided for by the relevant regulatory legal acts. Interference must have a legitimate aim. That is, such interference must be justified and aimed at achieving legitimate goals, such as protecting national security, maintaining public order, preventing crime, and so on. The intervention must be necessary within the framework of a democratic society. This means that restrictions on personal data must be proportionate and necessary to achieve a legitimate aim, as well as consistent with the principles of a democratic society. Thus, the right to personal data receives its protection in accordance with the practice of the ECHR in the framework of the right to

privacy. The concept of personal data includes any information relating to a particular person or a person that can be identified. The subject of personal data has a number of rights, including the right to access, modify, destroy and protect their personal data. However, these rights may be restricted in order to achieve a legitimate aim, provided that such restriction is in accordance with the law and is necessary in a democratic society.

Forms and methods of protecting the rights of the subject of personal data under the legislation of Kazakhstan

Kazakhstan has taken an important step in line with international standards by adopting the law of the Republic of Kazakhstan No. 94-V "On personal data and their protection" on May 21, 2013, which is a significant point [21]. This law establishes the basic principles and rules for the processing and protection of personal data in the country. The law of Kazakhstan takes into account the importance of protecting personal data and ensures the rights of citizens to the confidentiality and inviolability of their personal information. It defines the basic principles of data processing, such as the consent of the data subject, the appropriateness, and limitation of data collection, as well as the obligations of data controllers and the rights of data subjects to access, correct and delete their personal data. The law also contains mechanisms for monitoring and punishing violations of the rules for processing personal data. It provides administrative and criminal sanctions for persons who do not comply with the requirements of the law and abuse personal data. Today, in Kazakhstan, most public services are provided online, which means that the personal data of citizens is in the digital space from the moment they are born. The security of this data is the responsibility of governmental and quasi-governmental organizations.

The protection of the rights of the subject of personal data, as well as other subjective civil rights, is carried out using appropriate forms of protection and certain methods of protection. In this context, two forms of protection are usually distinguished: jurisdictional and non-jurisdictional. The jurisdictional form of protection is associated with the ability to apply to the competent courts or other bodies in order to protect their rights, including the right to the protection of personal data. The non-jurisdictional form of protection includes self-regulatory mechanisms, regulations and other means that may help protect the rights of personal data subjects. The non-jurisdictional form of protection of the rights of the subject of personal data is a special method of protection due to the informational nature of personal data. This form of protection has several features that should be considered. Firstly, a non-jurisdictional form of protection provides the subject of personal data with a priority right to self-defence. That is, the subject has the right to take measures to prevent violations of their rights and counter illegal interference. Such a right follows from the provisions of the Law of Kazakhstan "On Personal Data and Their Protection" and allows the subject to use various means of self-defence that are not prohibited by law and comply with the moral standards of society.

Examples of such self-protection measures include installing special software on a computer that blocks access to websites that use programs to illegally collect personal data. In addition, the subject of personal data may apply cryptographic protection methods, such as mathematical encryption algorithms, to ensure the security of transmission and storage of their data. Thus, the non-jurisdictional form of protection of the rights of the subject of personal data provides an opportunity for the subject to independently protect their rights and take measures to prevent and eliminate violations of their personal data. Given the relevance of personal data protection issues on the Internet, it is important to pay attention to the guidelines set out in the Council of Europe Committee Recommendation "On the Protection of Privacy on the Internet" [22]. These guidelines offer guidance to Internet users and service providers regarding how to behave online. In this context, it should be noted that Kazakh legislation provides not only the rights of personal data subjects to self-defence, but also the obligation of owners, processors of personal data and third parties to ensure their security. In accordance with these requirements, data is protected from accidental loss or destruction, illegal processing and illegal access to personal data. Kazakh norms fully comply with the European standards that were presented earlier. Thus, Kazakhstan takes serious measures to ensure the security of personal data and guarantees compliance with high standards in this area, meeting modern requirements and norms of the international community.

Therefore, owners, processors of personal data and third parties bear the risk of accidental infringement of the right to personal data. This is because personal data is considered confidential information, and its protection is aimed at preventing accidental or unauthorized damage, loss, as well as illegal access, modification, blocking, or transfer. In addition, in the process of processing personal data, there are certain risks for the rights and freedoms of data subjects related to their nature, scope, or purposes of processing, for example, depriving individuals of access to rights, services or contracts, as well as a result of the specific use of new technologies. In this regard, the responsibility for ensuring the established level of protection of personal data lies with the party distributing this data, as well as the party receiving personal data, which must take measures to protect them (Law of the Republic of Kazakhstan No. 94 -V "On personal data and their protection") [21].

Protection against such risks should be carried out at all stages of personal data processing with the help of organizational and technical measures. Organizational measures include: establishing rules for access to personal data for employees of the owner/manager; accounting for operations related to the processing of personal data and access to them; development of an action plan in case of unauthorized access to data, damage to technical equipment or emergency situations; regular training of employees working with personal data. Special technical security measures are applied to exclude unauthorized access to the processed personal data and ensure the safe operation of the hardware and software complex used to process personal data [23; 24]. As part of the processing of personal data, subjects are provided with an effective judicial remedy in case of violation of their rights by the owner or processor of personal data as a result of unlawful

processing (as per the provisions of Article 79 of the General Data Protection Regulation). This provides an opportunity for data subjects to go to court and protect their rights in case of violation of their personal data. This judicial remedy is an effective mechanism that guarantees data subjects access to judicial protection and the possibility of obtaining compensation in case of damage caused by the unlawful processing of their personal data. This is an important guarantee that ensures fairness and protection of the interests of data subjects in the digital environment [12; 25].

The jurisdictional form of protection implies the filing of an application, complaint, or other similar appeal by the subject of personal data to the competent state authority, including judicial authorities, which have the authority to take measures aimed at suppressing and preventing violations, restoring violated rights or compensating for damage caused. This form of protection may include general judicial procedure and special administrative procedures. The administrative form of personal data protection should be carried out by the activities of the authorized body, which has the competence and responsibilities in the field of personal data protection. It is necessary to provide two important opportunities in the functioning of the oversight body. Firstly, each data subject should be given the right to file a complaint with the supervisory authority in case of violation of the law in the processing of his personal data. Secondly, every natural or legal person must be guaranteed an effective remedy against a binding decision taken by the supervisory authority.

Thus, in the field of personal data protection, judicial protection is universal, since judicial jurisdiction extends to any disputes related to personal data. The right of the subject of personal data to judicial protection is guaranteed by the Constitution of the Republic of Kazakhstan (Article 13) [26]. One of the main ways of special protection of the right to personal data is the requirement to stop processing, change or destroy personal data. These claims can be brought both in the form of a judicial form of protection, and in the form of a non-jurisdictional procedure. For example, the subject of personal data has the right to object to the processing of his personal data. If such objections are justified, the owner of personal data must stop processing them. A justified request of the subject of personal data may lead to the termination of further processing and, consequently, the storage of data by the owner and manager. In such a case, the only legal consequence of such a requirement is the destruction of the relevant information.

However, the termination of the use of personal data may take various forms, including destruction, blocking or other methods. For example, UK direct marketing associations prefer to block rather than delete the data of citizens who have expressed their unwillingness to receive targeted promotional offers. This approach is due to the fact that deleted data can be mistakenly entered again into the system, which will require additional efforts from both citizens and associations to re-exclude data. An important precedent in the field of deletion and objection to the processing of personal data was the decision of the Court of Justice of the European Union of May 13, 2014 in the case of Google Spain SL, Google Inc. v. Spanish Data Protection Agency (AEPD), Mario Costeja González [27]. This decision has received wide attention and is considered significant in the context of the right to erasure of personal data (the right to be forgotten). Thus, the rules for changing or destroying personal data are clearly defined in Kazakhstani legislation, and their observance ensures the protection of the rights of personal data subjects.

Separately, it is necessary to consider the issue of compensation (compensation) for damage, both property and moral, caused by a violation of the right to personal data. It is important to note that the Law of the Republic of Kazakhstan "On the Protection of Personal Data" does not contain direct provisions establishing the right of the subject of personal data to receive compensation for such damage. This is not in line with European standards, including Article 82 of the General Data Protection Regulation and Article 23 of Directive 95/46/EC [11, 12], which provide for the right to compensation for any person who has suffered damage as a result of illegal processing or violation of the legislation on the protection of personal data by the owner or operator of personal data. However, this does not exclude the possibility of the subject of personal data to go to court and demand compensation for property and moral damage on the basis of general provisions, such as articles 951-952 of the Civil Code of the Republic of Kazakhstan [28].

Thus, the multidimensionality of the legal nature of the right to personal data as a subjective right, as well as the wide scope of the concept of "personal data" as an object of law, determine a complex system for protecting such data. The right to personal data, being a civil subjective right, can be protected using general civil law methods. Comparing the main regulatory documents of other countries and Kazakhstan, it is easy to see that for the most part they provide for the implementation of similar measures in the field of personal data protection. Firstly, the laws are aimed at protecting the interests of citizens and guaranteeing the full protection of their constitutional rights and freedoms in the field of information security. However, at the moment there is no actual data on legal statistics in the field of personal data protection in Kazakhstan, and it is necessary to openly and transparently develop the legal mechanism in this area.

Therefore, it is important to promote a culture of personal data protection, including notification of data breaches to subjects in order to establish trust and take responsibility for the collection, processing, and storage of personal data seriously. In general, the system of stakeholders involved in the processes related to the protection of personal data is extensive. Despite the presence of specialized departments, supervisory authorities and other participants in information processes, such as the collection, processing, storage and destruction of personal data, it is important to realize that almost all government bodies and their divisions, including committees and departments, have at least one database with which they work. Therefore, it is necessary to develop and implement effective measures to protect personal data that would ensure the confidentiality, integrity, and availability of information. This includes the adoption of appropriate laws and regulations, training and raising awareness among employees and the public about the importance of protecting personal data, and establishing

the technical means and infrastructure for reliable and secure processing of information. In addition, it is necessary to actively involve citizens in the process of protecting personal data, providing them with the ability to control and manage their personal data. This can be done through the development of convenient and transparent consent mechanisms for data processing, the ability to choose the level of confidentiality, as well as access to information about how and for what purposes their data is used. In general, the culture of personal data protection should become an integral part of daily life and social activities. It must be built into all aspects of the work of government bodies, business, and society in order to ensure a high level of trust and protection of the rights of citizens in the digital age.

The current system of personal data protection has its limitations, as it only covers certain types of data and relies on consent as the basis for the transfer of personal data [29; 30]. However, it does not fully satisfy the existing problems associated with unauthorized access to personal data and is not able to fully ensure the rights of citizens to their data in relation to their content, use, and control of the processing and sharing of data. Therefore, the authors consider it necessary to revise and update the rules for the protection of personal data, taking into account specific industries and their characteristics. These rules may focus on certain groups of workers and allow them to participate more actively, as well as employers to expand the scope of all relevant types of personal data and the scope of their transfer. To strengthen the protection of personal data in Kazakhstan and improve the digital ecosystem, the following areas can be considered when developing legislation:

1. Expanding scope: Legislation should be expanded to cover all types of personal data and establish mandatory protection measures for each type. It is necessary to take into account new technologies and the development of information systems in order for the legislation to remain relevant.
2. Establish clear rights and obligations: Legislation should clearly define the rights of workers in relation to their personal data, including the right to access, correct and delete their data. It should also establish responsibilities for organizations that process personal data, including requirements for security and data breach notification.
3. Establishing an independent data protection authority: It is important to consider establishing a dedicated authority or strengthening the role of existing authorities to oversee and enforce data protection laws. This body should have the power to investigate violations, impose fines and enforce workers' rights.
4. Training and awareness raising: in addition to legislative measures, it is important to conduct educational programs and campaigns to raise awareness among workers about the importance of protecting personal data and digital rights. This may include training in digital literacy, the basics of cybersecurity and understanding the risks associated with the processing of personal data.
5. International cooperation: Kazakhstan should actively participate in international initiatives and standardization in the field of personal data protection. This will help create a harmonized approach to data protection and establish trust from other countries and organizations.
6. Regular monitoring and updating: Legislation should be regularly monitored and updated to reflect changes in the technological and information environment. This allows legislators to respond to new challenges and threats in the field of personal data protection, as well as to adapt the provisions of the law to best practice and international standards. Regular monitoring and updating of legislation also contributes to its effective implementation and compliance with personal data protection requirements.

Analysis of existing problems and prospects for the legislative protection of personal data

In recent years, extensive research has been carried out aimed at the protection of personal data, and as a result, significant theoretical conclusions have been obtained. For example, D. Mangku et al. noted that with the growth in the number of mobile phone users and the Internet, the importance of protecting personal data is increasing [31]. Therefore, specific and comprehensive legislation governing the protection of personal data is required. A study by N. Fibrianti and A. Holish found that there is a legal vacuum in relation to the protection of consumer personal data in several applicable standard rules [32]. This is due to the lack of specific and comprehensive rules that would ensure the legal protection of consumer personal data.

According to G. Tataru and S. Tataru, the introduction of new data protection rules has a significant impact on society and resources [33]. In the current context, the rules set by the GDPR remind operators that people, including human resources as well as data, are not just objects to be exploited, but require accountability, transparency, and respect for human rights. Thus, scientists' research confirms the importance of the problem of personal data protection and the need to develop appropriate legislation to ensure legal protection and take into account the rights and interests of users and consumers. At the same time, it must be understood that too strict and detailed legislation in the field of personal data protection can negatively affect the development of innovation and the digital economy. Overregulation can restrict companies' freedom of action and restrict access to data, which in turn can hinder the development of new technologies and progress. It can also be argued that ensuring full protection of personal data may be next to impossible due to the rapidly changing technological environment and new threats constantly emerging. In addition, the individual responsibility of users in the field of data security also plays an important role and should not be completely shifted to government authorities and legislation [34; 35].

In a study conducted by B. Mittelstadt, it is noted that systems for the general collection of confidential personal data are currently being implemented [36]. However, it is doubtful that users are fully aware of the potential consequences of privacy breaches and data mining. According to V. Justickis, the role of balancing is of great importance in the protection of personal data [37]. This principle is widely applied by European courts to resolve disputes arising from the application of data protection rights. It also serves as a basis for the harmonization of

European and national legislation and is used to establish the right balance of interests between the European Union and the Member States. Balancing plays a critical role in the daily practice of data protection. The main data protection statute, the EU General Data Protection Regulation, states that balancing should be the main means of regulating the relationship between the right to data protection and other rights.

In this context, C. Labadie and C. Legner express the point of view that data protection rules provide a set of rights to individuals aimed at ensuring the transparency of data processing and a clear definition of the scope of data processing activities [38]. The inclusion of these rights means that organizations are required to comply with certain requirements. To do this, the concept of the process life cycle and business rules are used to show how these requirements affect data management practices. Thus, the researchers draw attention to the need for a conscious approach to the protection of personal data, taking into account the balancing of interests and the creation of transparent rules in order to ensure effective data protection and compliance with the principles of privacy. While there is general recognition of the importance of protecting personal data, one must be aware of the possible negative consequences of over-regulation and the limitations that may arise when developing strong legislation in this area. The balance between protecting data and stimulating innovation is a complex issue that requires further study and discussion.

Z. Sun and Z. Liu conclude that the protection of sensitive personal information should be strengthened and classified [39]. Existing laws, such as the Personal Information Protection Act, should be used as a guide, and the criminal law aspect should specify the acts, objects, scope, and criteria for criminalizing breaches of sensitive personal information. The EU General Data Protection Regulation (GDPR) is designed to provide a consolidated framework for regulating the commercial use of personal data and strengthening data protection for EU citizens. The GDPR aims to standardize and modernize data protection legislation related to the Internet, social media and the digital market, and to ensure and expand the rights of EU citizens regarding the privacy of their data. R. Carvalho et al. note that the transfer of control over personal data to individuals in the EU with the granting of new rights to EU data subjects has an impact on how organizations work with personal information [40]. And it is the GDPR that has changed the way personal information is collected and managed, including the definition of new roles in data organizations.

According to W. Obiagwu, the GDPR has significantly increased the awareness and control of citizens over their personal data and has significantly influenced data security policy around the world [41]. The regulation has also raised data protection standards, forcing tech giants to rethink their personal data practices and put more emphasis on privacy. However, effective implementation of the GDPR requires more use of the tools provided by the GDPR to facilitate the application of the rules. In fact, the concept of making data protection law more effective by requiring regulators to incorporate legal norms into the technical and organizational structure of data processing has been around for a long time. Data protection and privacy issues have been discussed for many years. However, there has recently been a shift towards including data protection within the law, and the full implications of this approach have not yet been fully explored. According to Article 25 of the General Data Protection Regulation, the subjects of regulation are obliged not only to implement the legal provisions in the structure of data processing, but also to do so efficiently. By explicitly requiring the effectiveness of protective measures as a mandatory result, the legislator inevitably raises the question of methods for verifying and ensuring effectiveness. In fact, the extension of legal compliance assessment to the real consequences of the required measures opens up the possibility of using (non-legal) methodologies that specialize in the empirical evaluation of data protection measures [42; 43].

According to Ö. Ozkan et al., the new Turkish personal data protection law raises problems as a wide variety of information is widely collected and exceptions are numerous [44]. The importance of the consent of the data subject is ignored, even in relation to sensitive information. Such a variety of data is collected about sex life that almost everything can be included. The ruling was published after the personal data protection law received a lot of negative feedback from stakeholders. There are no restrictions on data collection in law, so all kinds of data can be collected. Some issues identified in the implementation of the Brazilian Data Protection Law are related to the need for legal adjustments and related training, the development of a complete action plan for companies to comply with the LGPD, the specialized implementation of personal data management processes, the application of information protection technologies, informing the Brazilian public about it Law, as well as demonstration of the rights and obligations of citizens. Therefore, according to J. Souza et al., there will be a lot of debate and discussion regarding the LGPD and its compliance with the General Data Protection Regulation (GDPR), as well as issues related to the application of current legislation in Brazil [45].

S. Quach et al. emphasize that research is needed to understand how new digital technologies, including artificial intelligence, can pose a threat to the privacy of consumer information, individual risks and privacy risks during interaction with data [46]. Such research can explore consumer perceptions of firms' data use strategies (such as data collection, awareness, support, and expertise), actual data privacy practices, and levels of regulation, which can ultimately help create long-term, technology-based outcomes for all stakeholders. The critical issue is to define consumer segments and achieve data processing trade-offs that are more acceptable to them. Consumers adopt various forms of protection against privacy risks, both reactive and proactive [47-49]. R. Ducato also emphasizes that scientific research is one of the areas in which Member States can intervene with specific provisions to improve the protection of personal data both at the EU level and at the national level [50]. In this context, strict adherence to the principles of personal data protection is a key element in ensuring the protection of personal rights. Moreover, their due observance will stop the practice of unconditional collection and use of such data and create conditions for high-quality processing of personal data.

To increase the level of security, it is necessary that not only those who directly have the authority to control personal data, but also all participants in data protection processes are well aware of the principles and can effectively apply them. Their deep understanding is necessary not only to assess violations in data processing, but also to determine the fact of violation of the rights of an individual. The Principles for the Protection of Personal Data set out the framework for the application of the legal framework, regulating the collection and processing of personal data, and also serve as a basis for resolving disputes between competing rights. They can help avoid restrictions on the transfer of personal data across borders between EU Member States with different standards and reduce the risk of personal data abuse directly in the Republic of Kazakhstan.

Conclusions

The right to personal data, being a subjective civil right, can be protected by applying general civil law methods. Within the framework of general civil law ways of protecting the right to personal data, the consent of the data subject, the principles of expediency and limitation of data collection, as well as the obligations of data controllers are important elements. The consent of the data subject is a key factor for the legitimacy of the processing and use of his personal data, and the principles of expediency and limitation of data collection help ensure that personal data is collected and used only within the established purposes and with a limited amount of information. General civil law methods for protecting the right to personal data serve as the basis for ensuring a fair and effective system for protecting personal data. They provide data subjects with the tools to control their personal information and ensure that data operators are held accountable for compliance with the rules for processing personal data. As a result, the right to personal data is a subjective civil right, and its protection requires the application of general civil law methods that ensure that the principles of expediency, limitation of data collection and obligations of data operators are observed.

International and European law currently provides for preventive measures within the framework of regulatory relations aimed at preventing violations of the rights of personal data subjects in the future. In some countries, laws are enacted that give certain individuals control over the collection, processing, and transfer of personal data to public and private organizations due to the widespread and increased threat to the security of personal data. The practice of the European Court of Human Rights has led to the development of criteria for the lawful restriction of rights to personal data, which are consistent with the general principles of lawful interference with privacy. The adoption of the Law "On Personal Data and their Protection" in Kazakhstan made it possible to harmonize legal regulation in the field of personal data protection with international standards and ensure a high level of confidentiality and security of personal data of citizens. This contributes to strengthening public confidence in the digital economy and electronic services, and also contributes to the development of information exchange and digital innovation in the country. In general, the adoption of this law confirms Kazakhstan's desire for a modern and efficient personal data protection system that meets modern requirements and ensures the rights and interests of citizens in the processing and use of their personal information.

Currently, the existing personal data protection system has its limitations and is applicable only to certain types of information. It relies on consent as the legal basis for the transfer of personal data, but it does not provide full coverage of work-related issues, which in turn limits the exercise of workers' rights to the content, processing, and control of their data, as well as their sharing. Therefore, it is important to understand that the development and adoption of specialized legislation, the delegation of authority or the creation of special bodies, as well as promotion in the ratings of Internet freedom or cybersecurity are only the initial steps towards creating a sustainable digital ecosystem. For Kazakhstan, which is actively digitalizing in order to integrate into global information processes, in addition to legislative initiatives regulating this area, it is also important to focus on raising employee awareness of the importance of protecting personal data and promoting digital rights by deepening knowledge and developing digital literacy among employees.

Acknowledgements

None.

Conflict of Interest

None.

References

[1] Dzhaksylykov A. Personal data protection in Kazakhstan: Status, risks and opportunities. 2020. https://www.soros.kz/wp-content/uploads/2020/04/Personal_data_report.pdf

[2] Center for Analysis and Investigation of Cyberattacks, Kazakhstan. Register of databases of information leaks in Kazakhstan. 2022. https://cert.kz/novosti/data-leak-register

[3] Order of the Minister of Digital Development, Innovation, and Aerospace Industry of the Republic of Kazakhstan No. 395/HK "On approval of the Rules for the collection and processing of personal data". 2020. https://online.zakon.kz/Document/?doc_id=39051375

[4] Akmalovich AS. International legal regulation of personal data protection on the global internet. *J Law Res.* 2023;1:88-97.

[5] Akhambaev R, Akhmetova Zh. Recommendations and norms for the protection of personal data in corporate information systems. *Bull KazATC*. 2019;2:156-162.

[6] Maksutov B. Activities of an independent body for the protection of personal data in the Republic of Kazakhstan. In: *Collection of Scientific Articles IX International Correspondence Scientific Specialized Conference* (pp. 56-68). Boston: Problems of Science; 2019.

[7] Syrlybaeva FM. Some issues of protection of employee information rights. *Bull L.N. Gumilyov Eurasian Nation Uni*. 2022;3(140):72-80.
[8] Bissaliyev MS, Shakirov KN. Digital footprints as a factor in the security of personal data trafficking on the Internet. *Bull L.N. Gumilyov Eurasian Nation Uni*. 2023;1:81-98.
[9] European Convention on Human Rights. 1950. https://www.echr.coe.int/documents/convention_rus.pdf
[10] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. 1981. https://rm.coe.int/1680078c46
[11] Directive of the European Parliament and of the Council No. 2002/58/EC "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data". 1995. http://consultant.parus.ua/?doc=08EHE16107&abz=E2E01
[12] Regulation of the European Parliament and of the Council No. 2016/679 "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data". 2016. http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=ENм
[13] United Nations. UN Study: E-Government. 2022. https://desapublications.un.org/sites/default/files/publications/2023-02/UN%20E-Government%20Survey%202022%20-%20Russian%20Web%20Version.pdf
[14] Klosowski T. The State of Consumer Data Privacy Laws in the US (And Why It Matters). 2021. https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/
[15] General Personal Data Protection Act of Brazil. 2020. https://lgpd-brazil.info/
[16] Souza J, Abe J, Lima L, Souza N. The general law principles for protection the personal data and their importance. In: *Computer Science & Information Technology* (pp. 109-120). Chennai: AIRCC; 2020.
[17] Freedom House. Freedom in the world. 2022. https://freedomhouse.org/sites/default/files/2022-02/FIW_2022_PDF_Booklet_Digital_Final_Web.pdf
[18] European Court of Human Rights. Case of Amann v. Switzerland, App. No. 27798/95. 1992. http://hudoc.echr.coe.int/eng?i=001-58497
[19] European Court of Human Rights. Case of Leander v. Sweden, App. No. 9248/81. 1987. http://hudoc.echr.coe.int/eng?i=001-57519
[20] European Court of Human Rights. Case of Rotaru v. Romania, App. No. 28341/95. 1995. http://hudoc.echr.coe.int/eng?i=001-58586
[21] Law of the Republic of Kazakhstan No. 94-V "On personal data and their protection". 2013. https://online.zakon.kz/Document/?doc_id=31396226&pos=3;-108#pos=3;-108
[22] Council of Europe Committee Recommendation "On the Protection of Privacy on the Internet". 1999. https://www.refworld.org.ru/publisher,COEMINISTERS,,,5511791b4,0.html
[23] Abdymanapov SA, Muratbekov M, Altynbek S, Barlybayev A. Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems. *IEEE Acc*. 2021;9:156556-156565.
[24] Pirahandeh M, Kim D-H. A New Energy-Aware GPU Based Erasure Coding Scheduler for Cloud Storage Systems. *Int Conf Ubiquit Fut Network ICUFN*. 2018;2018:619-621.
[25] Spytska L. The Nature of Sexual Violence: The Criminological Concept of Victimisation. *Pak J Crim.* 2023;15(4):1-20.
[26] Constitution of the Republic of Kazakhstan. 1926. https://www.akorda.kz/ru/official_documents/constitution
[27] Google Spain SL, Google Inc. v. Agencia Espanola de Protection de Datos (AEPD), Mario Costeja Gonzalez, Case C-131/12. 2014. http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en
[28] Civil Code of the Republic of Kazakhstan. 1994. https://online.zakon.kz/Document/?doc_id=1006061
[29] Cherniha R, Serov M. Nonlinear systems of the Burgers-type equations: Lie and Q-conditional symmetries, Ansätze and solutions. *J Mathem Analys Appl.* 2003;282(1):305-328.
[30] Barlybayev A, Sankibayev A, Kadyr Y, Amangeldy N, Sabyrov T. Predicting Used-Vehicle Resale Value in Developing Markets: Application of Machine Learning Models to the Kazakhstan Car Market. *Ing Syst d'Inf.* 2023;28(5):1237-1246.
[31] Mangku D, Yuliartini N, Suastika I, Wirawan G. The personal data protection of internet users in Indonesia. *J Southwest Jiaton Uni*. 2020;56(1):202-209.
[32] Fibrianti N, Holish A. Consumer personal data protection: Between expectations and reality. 2021. https://eudl.eu/pdf/10.4108/eai.8-6-2021.2314376
[33] Tataru G, Tataru S. Human resources and personal data protection: An indissoluble relationship. *J Pub Admin, Fin Law*. 2020;18:303-311.
[34] Trus I, Gomelya N, Halysh V, Radovenchyk I, Stepova O, Levytska O. Technology of the comprehensive desalination of wastewater from mines. *East-Eur J Enter Tech*. 2020;3(6-105):21-27.
[35] Rehman HU, Darus M, Salah J. Generalizing Certain Analytic Functions Correlative to the n -th Coefficient of Certain Class of Bi-Univalent Functions. *J Mathem*. 2021;2021:6621315.
[36] Mittelstadt B. Personal Data Protection. 2013. https://www.academia.edu/3749876/Personal_Data_Protection
[37] Justickis V. Balancing personal data protection with other human rights and public interest: between theory and practice. *Baltic J Law Polit*. 2020;13:140-162.
[38] Labadie C, Legner C. Personal data management inside and out. *Enterp Model Info Syst Archit*. 2020;15(9). https://doi.org/10.18417/emisa.15.9

[39] Sun Z, Liu Z. Inadequacy and improvement of legal protection of sensitive personal information. *Int Conf Educ Sci Social Cult*. 2023;157:03006.
[40] Carvalho RM, del Prete C, Martin YS, Rivero RM, Önen M, Schiavo FP, Rumin AC, Mouratidis H, Yelmo JC, Koukovini MN. Protecting citizens' personal data and privacy: Joint effort from GDPR EU cluster research projects. *SN Comp Sci*. 2020;1:217.
[41] Obiagwu W. How the GDPR protects personal data in the digital age. *ELSA Austr Law Rev*. 2022;1:25-31.
[42] Grafenstein M, Jakobi T, Stevens G. Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-centred UX-design methods. *Comp Law Secur Rev*. 2022;46:105722.
[43] Spytska LV. Analysis of the most unusual court decisions in the world practice in terms of the right to justice. *Soc Leg Stud*. 2022;5(4):39-45.
[44] Özkan Ö, Şahinol M, Aydinoglu AU, Son YA. Reflections on Turkish personal data protection law and genetic data in focus group discussions. *NanoEthic*. 2023;16:297-312.
[45] Souza J, Abe JM, de Lima LA, de Souza NA. The Brazilian law on personal data protection. *Int J Network Secur Its Appl*. 2020;12(6):15-25.
[46] Quach S, Thaichon P, Martin KD, Weaven S, Palmtier RW. Digital technologies: Tensions in privacy and data. *J Academ Market Sci*. 2022;50:1299-1323.
[47] Azizov TN, Kochkarev DV, Galinska TA. New design concepts for strengthening of continuous reinforced-concrete beams. *IOP Conf Ser: Mater Sci Eng.* 2019;708(1):012040.
[48] Buil R, Piera MA, Ginters E. Multi-agent system simulation for urban policy design: Open space land use change problem. *Int J Mod Simul Sci Comput*. 2016;7(2):1642002.
[49] Ginters E, Dimitrovs E. Latent Impacts on Digital Technologies Sustainability Assessment and Development. *Adv Intell Syst Comput.* 2021;1365:3-13.
[50] Ducato R. Data protection, scientific research, and the role of information. *Comp Law Secur Rev*. 2020;37:105412.

Легальні способи та методи захисту персональних даних в Казахстані

Алмас Аміров
Академія правоохоронних органів при Генеральній прокуратурі Республіки Казахстан
010078, вул. Республіки, 94, м. Коси, Республіка Казахстан

Даріга Кайназарова
Академія правоохоронних органів при Генеральній прокуратурі Республіки Казахстан
010078, вул. Республіки, 94, м. Коси, Республіка Казахстан

Ернар Бегалієв
Академія правоохоронних органів при Генеральній прокуратурі Республіки Казахстан
010078, вул. Республіки, 94, м. Коси, Республіка Казахстан

Азамат Сарсенбаєв
Академія правоохоронних органів при Генеральній прокуратурі Республіки Казахстан
010078, вул. Республіки, 94, м. Коси, Республіка Казахстан

Нурлибек Сарибаєв
Академія правоохоронних органів при Генеральній прокуратурі Республіки Казахстан
010078, вул. Республіки, 94, м. Коси, Республіка Казахстан

Анотація

Актуальність. Актуальність дослідження полягає в необхідності розвитку теоретичних уявлень з цього питання та визначення перспективних напрямів імплементації в законодавство Республіки Казахстан, яке на сьогодні не є досконалим у контексті правового регулювання захисту персональних даних.

Мета. Метою дослідження є вивчення особливостей захисту персональних даних у Республіці Казахстан та інших країнах (країнах Європейського Союзу, Сполучених Штатах Америки, Бразилії).

Методологія. Методологічною основою статті стали методи статистичного аналізу, аналогії та узагальнення, а також порівняльно-правовий, формально-юридичний та формально-логічний методи.

Результати. Дослідження виявило особливості правового регулювання захисту персональних даних за законодавством Республіки Казахстан. Крім того, встановлено, що законодавство Європейського Союзу містить додаткові зобов'язання, які спрямовані на максимальний захист персональних даних. Однак чинне законодавство Казахстану є фрагментарним і не в повній мірі приділяє належну увагу питанням захисту персональних даних. У зв'язку з цим було запропоновано переглянути і оновити правила захисту персональних даних для конкретних галузей з урахуванням їх специфіки. Крім того, наголошено на важливості підвищення обізнаності громадян щодо прав та обов'язків у цифровій сфері, що включає популяризацію знань про безпечне користування Інтернетом, засоби захисту персональних даних та кібергігієну.

Висновки. Відзначено роль активної співпраці з міжнародними партнерами та організаціями, що сприятиме обміну досвідом та кращими практиками у сфері цифрової безпеки та захисту персональних даних. Регулярні огляди та перегляд існуючих механізмів захисту, а також впровадження нових технологічних рішень та інновацій сприятимуть забезпеченню стійкої та надійної цифрової екосистеми в довгостроковій перспективі.

Ключові слова: інформаційна безпека; конфіденційність; приватність; глобальна мережа Інтернет; досвід Європейського Союзу.