УДК 34.096
МРНТИ 10.27.51

DOI: https://doi.org/10.37788/2025-1/173-178

O.B. Dubovitskaya[1*]
[1]Toraygirov University, Kazakhstan
*(e-mail: o.b.d.1970@mail.ru)

Establishment and development of the personal data protection institute

Abstract

*Main Problem***:** The article addresses the issue of personal data protection in the context of technological advancements and the risks of data leaks, as well as the insufficient effectiveness of legislation, especially in Kazakhstan.

Objective: The aim of the research is to analyze the development of the personal data protection institution globally and in Kazakhstan, evaluating existing approaches and challenges in legal regulation.

Methods: The methods used include analyzing regulatory documents, evaluating research from Kazakhstan's ministries, and comparing international practices in personal data protection.

*Results and their value***:** currently: The results show that personal data protection is a crucial part of human rights and requires improvement in legislation, especially in Kazakhstan. Issues of data leaks and weaknesses in protection need to be addressed, including the establishment of effective agencies and increasing public awareness of cybersecurity.

Keywords: personal data protection, cybersecurity, legislation, data leaks, human rights.

Introduction

The issue of protecting personal data of individuals has been a pressing concern for the global community for as long as humanity has existed. In the modern world, the right to privacy is enshrined in the constitutions of all developed countries. This right means that only the individual, who possesses certain information about themselves, has the right to decide whether or not to disclose it. It should be noted that the legislation of many countries also establishes a list of entities that have the right to require the disclosure of an individual's personal data. If there is an unlawful disclosure of such information, the owner of the data is entitled to protect their violated interests, and the measures of responsibility for the harm caused are not always limited to civil liability [1]. In some countries, including Kazakhstan, the unlawful disclosure of certain personal data is considered a criminal offense [2].

Materials and Methods

The materials and methods of the research include the analysis of regulatory legal acts, research published by the Ministry of Digital Development, Defense, and Aerospace Industry of the Republic of Kazakhstan, as well as the evaluation of existing approaches to personal data protection, information processing, and regulation in the field of cybersecurity.

Results

If we look at the history of the development of the institute of personal data protection, it is primarily associated with the period of the French Revolution. Historians note that the concept of protecting personal data as a universal humanitarian concept began during the French Revolution. It was during this period that the concept was proclaimed, which led to the identification of the individual as such and the prioritization of their interests over those of an unlimited state. Later, the understanding of the right to privacy was formed, one of the components of which was the right to protect personal information. This inalienable right of the individual is protected from illegal encroachments by both the state and third parties. In its development towards the formation of the concept of personal data, the idea passed through a stage of existence as personal human rights. These rights include: a) the right to receive information concerning the individual's interests; b) the right to protect data related to private life.

Discussion

The history of personal data as a concept and its protection begins in the United States at the end of the 19th century. It was then that the legal category of "privacy" and its legal protection were

formed. "Privacy" generally refers to the inviolability of private life. In 1890, two American lawyers, Samuel Warren and Louis Brandeis, defined this concept as "the right to be alone"—the right to be left alone or the right to be left to oneself [3]. They argued that the development of business and the emergence of new methods of conducting entrepreneurial activity created opportunities for infringing on the inalienable rights of individuals. The progress of information technology further heightened this danger.

This theoretical concept quickly found support in legal practice. In the courts of the Anglo-Saxon legal system, by the 1960s, the right to privacy was derived from the first five amendments to the U.S. Constitution. A judge who made this ruling recognized that the right to privacy, and thus the protection of personal data, existed before the Bill of Rights [3].

The American concept of privacy, including the protection of personal data, laid the foundation for Article 12 of the Universal Declaration of Human Rights, adopted by the UN in 1948 [4]. This article stated that no one, except by lawful court order or decision of authorized bodies, could infringe on the privacy of personal life and correspondence.

After the 1960s-70s, when personal computers were actively used in business and government bodies to process various data, including confidential data such as personal data, the question of their legal regulation arose. There was a need to establish universally accepted rules for processing and transmitting personal data through telecommunications channels. The European Union and the European Commission quickly recognized the seriousness of the problem and began developing their own directives specifically regulating personal data protection.

The first significant document was the Convention adopted by the Council of Europe in 1981, dedicated to the protection of the rights and freedoms of individuals in the automatic processing of their personal data [5]. The protection of data was identified as an essential part of the right to privacy in its American understanding. Its protection was to be carried out within the general framework of human rights protection. However, this document was of a framework nature, setting the main directions for regulatory work, including methods of hardware processing and technical means used. In response to this societal demand, the European Union adopted Directive 95/46/EC in 1995, which addressed the processing of personal data and their free movement, including transborder transfer.

It can be confidently stated that the standards developed by European lawmakers were widely accepted around the world, as they offered highly detailed and clear regulation of personal data protection. Later, in 2000, the European Charter of Fundamental Rights was adopted, in which personal data and the right to their protection were proclaimed as fundamental values [6].

After the formation of fundamental regulatory acts defining general concepts and standards, the period began when individual national laws were developed, not only by countries but also by smaller administrative-territorial units. The first law regulating this area was the law on personal data protection in the German state of Hesse, passed in 1970. After the creation of the first practical application of this law, approximately 20 more laws were passed by other countries and provinces in Europe. These documents implemented real practical mechanisms for protecting the personal rights of citizens.

The 1990s were characterized by rapid automation of information processing processes and increasing demands from European and American societies to establish standards for the safe processing of personal data, excluding leaks, unlawful dissemination, or misuse.

In Russia, the concept of the right to privacy and the secrecy of correspondence has a long history. The Postal Statute adopted in 1857 during the reign of Alexander II, and the Telegraph Statute that came into force in 1876, proclaimed the secrecy of correspondence. This was protected under criminal law, with penalties for violating the confidentiality of messages. Interestingly, under the 1903 Criminal Code, even government officials could be held accountable if they interfered with the private lives of citizens during the performance of their duties related to administering justice [7].

However, this concept of privacy regulation was rendered obsolete after the 1917 revolution, which abolished all previously adopted laws, including those related to the protection of personal data and the secrecy of private life and correspondence. The 1918 Constitution contained a section on human rights, but it was primarily declarative in nature, reflecting the wartime and revolutionary period. It did not include most of the achievements of European democracy concerning human rights, only acknowledging: a) protection from exploiters; b) participation in governance; c) the right to free land use.

At this time, the inviolability of private life was not addressed, as the principle of war communism excluded any individualism. The 1924 USSR Constitution also did not address private

life. Personal data protection, privacy, and the right to correspondence were not regarded as grounds for deviation from communist ideology. However, history continued to evolve, and soon this aspect of human interests was given attention. The 1936 Stalin Constitution introduced a section entirely dedicated to the rights and freedoms of citizens. Articles 127-128 of this document addressed the inviolability of the person, inviolability of the home, and the secrecy of correspondence. The adoption of this Constitution was a significant achievement for Soviet legal theory, but in practical terms, many of these norms, including those regarding personal data protection, were largely formal. For instance, the right to the secrecy of telephone conversations was completely eliminated with a decree from the NKVD requiring the stenography of all telephone conversations of embassy staff and international organizations. Additionally, a mandatory censorship of all correspondence was introduced if the addressee was in another country. In the 1940s, during wartime, the issue of privacy and the secrecy of correspondence was entirely removed from the agenda [3].

The 1950s-60s in the USSR marked a period of "thaw." The country began to actively embrace international humanitarian values. After the ratification of the 1966 International Covenant on Civil and Political Rights, a new Constitution was developed, fully reflecting the evolving practice of protecting information rights, including the right to personal data protection. The respect for the individual was proclaimed as an important duty of government bodies and officials. Citizens were granted the right to inviolability: a) of the person; b) of the home; c) of correspondence, telephone conversations, and telegraph messages.

In 1999, the Assembly of the CIS countries adopted a model law on personal data protection, providing member states with the basic terms and rules for regulating the field. It was intended to serve as a basis for national legislation. In practice, Russia largely adopted the European approach, which became the foundation for the creation of the "Personal Data" law. In terms of protecting the rights of company personnel, relevant provisions from the International Labour Organization (ILO) recommendations were incorporated into the Labour Code [3].

In Kazakhstan, the Law "On Personal Data and Their Protection" (hereinafter referred to as the Law) was adopted on May 21, 2013. Like any other law, it includes terminology and the main directions of personal data protection. According to the law, "personal data refers to information relating to an identified or identifiable subject of personal data, recorded on electronic, paper, and/or other material carriers" [8]. The primary goal of this law is "to ensure the protection of the rights and freedoms of individuals when collecting and processing their personal data" [8], although storage is not mentioned.

Comparing this document with similar laws in other countries, it can be noted that, on the one hand, it is quite straightforward and comprehensive, but on the other hand, some aspects of personal data protection remain underdeveloped in practice. For example, Article 20 of the Law states that personal data is subject to protection, with the state acting as its guarantor.

Considering the large-scale data breaches in Kazakhstan in 2019 from the Central Election Commission and the Prosecutor General's Office databases, the question arises: how can the state guarantee the protection of personal information if, according to the Central Asian Registry of Cybersecurity (CARCA), the leak occurred from the database of the Prosecutor General's Office of the Republic of Kazakhstan, an authorized body in the field of personal data protection, and the Ministry of Internal Affairs of Kazakhstan suspended the investigation into the data breach due to the lack of a criminal case, arguing that "the mentioned information with data about citizens of Kazakhstan was not found on the Internet" [9].

The information about the personal data breach in Kazakhstan, according to the Ministry of Digital Development, Defense, and Aerospace Industry of the Republic of Kazakhstan, reveals several issues. Firstly, "each government body that owns databases is responsible for the security of its databases and compliance with the norms and rules for using and protecting the confidentiality of the information stored there" [10]. Secondly, no government body has the competence or authority to monitor the internet for violations of laws related to personal data protection. Thirdly, the country lacks a specialized body for personal data protection (analogous to the European Data Protection Agency).

Conclusion

In conclusion, it should be noted that over the past eight years, Kazakhstan has made significant progress in understanding, identifying, and addressing issues related to the use of cyber technologies in cyberspace. This has been reflected in Kazakhstan's position in the global cybersecurity index. However, alongside important initiatives and measures, the government and

society still face many tasks to be ready to recover as quickly as possible after cyberattacks, as preventing them is not feasible. Therefore, it is essential to develop a culture of personal data protection and not violate fundamental human rights and freedoms in both the online and offline worlds. As the saying goes, "forewarned is forearmed."

It is also worth mentioning that the government of Kazakhstan should pay more attention to raising awareness and knowledge among citizens regarding digital rights and personal data protection, enhancing the capacity of Kazakhstan's human rights organizations and researchers, and strengthening cooperation with partner institutions that have vast experience in this field. Cyber literacy and cyber hygiene should become an integral part of the campaign to promote a culture of personal data protection in Kazakhstan.

THE LIST OF SOURCES

1 Горохова Д.И. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных //Национальная безопасность 1(24) – 2013. [Электронный ресурс]. – URL: https://www.hse.ru/data/2013/03/11/1293471659/23394%20%D0%94.%D0%98.%20%D0%93% D0%BE%D1%80%D0%BE%D1%85% D0%BE%D0%B2%D0%B0.pdf.
2 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 12.09.2022 г.). [Электронный ресурс]. – URL: https://online.zakon.kz/document/?doc_id=31575252&pos=159;-52#pos=159;-52.
3 Важорова, М.А. История возникновения и становления института персональных данных / М.А. Важорова. – Текст : непосредственный // Государство и право: теория и практика: материалы I Междунар. науч. конф. (г. Челябинск, апрель 2011 г.). – Челябинск: Два комсомольца, 2011. – С. 33-38. [Электронный ресурс]. – URL: https://moluch.ru/conf/law/archive/37/365/.
4 Всеобщая декларация прав человека («Международный пакт о правах человека») от 10 декабря 1948 года. [Электронный ресурс]. – URL: https://adilet.zan.kz/rus/docs/O4800000001.
5 Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) (с изменениями от 15 июня 1999 г.). [Электронный ресурс]. – URL: https://online.zakon.kz/Document/?doc_id=1034061.
6 Вельдер И.А. Система правовой защиты персональных данных в Европейском союзе: Автореф. дис. канд. юрид.наук. Казань. 2006. – 27 с.
7 Глушкова С.И. Права человека в России: теория, история, практика: учеб. Пособие. Екатеринбург. 2002. – 748 с.
8 Закон Республики Казахстан от 21 мая 2013 года № 94-V «О персональных данных и их защите» (с изменениями и дополнениями по состоянию на 14.07.2022 г.). [Электронный ресурс]. – URL: https://online.zakon.kz/Document/?doc_id=31396226&pos=128;-45#pos=128;-45.
9 Официальный аккаунт ЦАРКА в Facebook. [Электронный ресурс]. – URL: https://m.facebook.com/story.php?story_fbid=2636221533272242&id=1674347306126341.
10 «Насколько казахстанцы защищены от утечки персональных данных», Profit, July 11, 2019. [Электронный ресурс]. – URL: https://profit.kz/news/53478/Naskolko-kazahstanci-zaschischeni-ot-utechki-personalnih-dannih/.

REFERENCE

1 Gorokhova D.I. (2013). Council of Europe Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data. National Security, 1(24), 1-11. Retrieved from https://www.hse.ru/data/2013/03/11/1293471659/23394%20%D0%94.%D0%98.%20%D0%93%D0%BE%D1%80%D0%BE%D1%85%D0%BE%D0%B2%D0%B0.pdf [in Russian].
2 Criminal Code of the Republic of Kazakhstan of July 3, 2014 No. 226-V (as amended and supplemented as of September 12, 2022). Retrieved from https://online.zakon.kz/document/?doc_id=31575252&pos=159;-52#pos=159;-52 [in Kazakh].
3 Vazhrova, M.A. (2011). The History of the Emergence and Development of the Institute of Personal Data. State and Law: Theory and Practice: Materials of the I International Scientific Conference (Chelyabinsk, April 2011), 33-38. Retrieved from https://moluch.ru/conf/law/archive/37/365/ [in Russian].

4 Universal Declaration of Human Rights (“International Covenant on Civil and Political Rights”) of December 10, 1948. Retrieved from https://adilet.zan.kz/rus/docs/O4800000001 [in English].
5 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Strasbourg, January 28, 1981) (as amended on June 15, 1999). Retrieved from https://online.zakon.kz/Document/?doc_id=1034061 [in English].
6 Velder, I.A. (2006). The System of Legal Protection of Personal Data in the European Union: Author’s Abstract of PhD Dissertation in Law. Kazan: Kazan University [in Russian].
7 Glushkova, S.I. (2002). Human Rights in Russia: Theory, History, Practice. Ekaterinburg: Ekaterinburg Publishing [in Russian].
8 Law of the Republic of Kazakhstan of May 21, 2013 No. 94-V "On Personal Data and Their Protection" (as amended and supplemented as of July 14, 2022). Retrieved from https://online.zakon.kz/Document/?doc_id=31396226&pos=128;-45#pos=128;-45 [in Kazakh].
9 Official account of the Central Asia Region Cybersecurity Agency on Facebook. Retrieved from https://m.facebook.com/story.php?story_fbid=2636221533272242&id=1674347306126341 [in English].
10 How Protected Are Kazakhstanis from Personal Data Leaks, Profit, July 11, 2019. Retrieved from https://profit.kz/news/53478/Naskolko-kazahstanci-zaschischeni-ot-utechki-personalnih-dannih/ [in Kazakh].

О.Б. Дубовицкая[1]
[1]Торайғыров университеті, Қазақстан

Жеке деректерді қорғау институтын құру және дамыту

Мақала жеке деректерді қорғау мәселесін технологиялық жетістіктер мен деректердің ағып кету қауіптері контексінде, сондай-ақ Қазақстандағы заңнаманың тиімділігінің жеткіліксіздігін қарастырады.

Зерттеудің мақсаты — жеке деректерді қорғау институтының дамуын әлемде және Қазақстанда талдау, қолданыстағы тәсілдер мен құқықтық реттеу саласындағы мәселелерді бағалау.

Зерттеуде нормативтік құжаттарды талдау, Қазақстанның министрліктері жасаған зерттеулерді бағалау және халықаралық жеке деректерді қорғау тәжірибелерін салыстыру әдістері қолданылады.

Нәтижелер көрсеткендей, жеке деректерді қорғау адам құқықтарының маңызды бөлігі болып табылады және заңнаманы жетілдіруді талап етеді, әсіресе Қазақстанда. Деректердің ағып кетуі және қорғаудың әлсіз тұстары шешілуі тиіс, соның ішінде тиімді агенттіктер құру және қоғамды киберқауіпсіздік туралы хабардар етуді арттыру қажет.

Түйін сөздер: жеке деректерді қорғау, киберқауіпсіздік, заңнама, деректердің ағып кетуі, адам құқықтары.

О.Б. Дубовицкая[1]
[1]Торайгыров университет, Казахстан

Создание и развитие института защиты персональных данных

Статья рассматривает проблему защиты персональных данных в контексте технологических достижений и рисков утечек данных, а также недостаточную эффективность законодательства, особенно в Казахстане.

Цель исследования – проанализировать развитие института защиты персональных данных на глобальном уровне и в Казахстане, оценить существующие подходы и проблемы в правовом регулировании.

В исследовании используются методы анализа нормативных документов, оценки исследований министерств Казахстана и сравнения международных практик защиты персональных данных.

Результаты показывают, что защита персональных данных является важной частью прав человека и требует совершенствования законодательства, особенно в Казахстане.

Проблемы утечек данных и недостатков в защите необходимо решить, включая создание эффективных агентств и повышение осведомленности общественности о кибербезопасности.

Ключевые слова: защита персональных данных, кибербезопасность, законодательство, утечка данных, права человека.

Date of receipt of the manuscript to the editor: 2025/01/06