CENTRAL ASIAN PERSPECTIVES OF PERSONAL DATA PROTECTION (CASE OF KAZAKHSTAN)

[1]ZHYLDYZ TEGIZBEKOVA, [2]TALGAT SARSENBAYEV

[1]Professor School of Law and Public Administration, Narxoz University, Almaty, Kazakhstan
[2]Professor, Director School of Law and Public Administration, Narxoz University, Almaty, Kazakhstan
E-mail: [1]zhyldyz.tegizbekova@narxoz.kz, [2]talgat.sarsenbayev@narxoz.kz

Abstract - The article examines the development and current state of personal data protection in Kazakhstan using a typical regional example. The study highlights that despite Kazakhstan's significant step toward modernization, including digital governance strategies and the establishment of regulatory bodies, personal data protection remains hampered by weak oversight and absence of an independent government oversight body.

Keywords - Kazakhstan, Personal Data, Biometrics, Artificial Intelligence, Legislation, Digital Code.

I. INTRODUCTION

The issue of personal data protection in Kazakhstan is more relevant today than ever before. We live in an era of digitalisation where information is becoming the main resource. Government agencies, businesses, educational and medical organisations are increasingly moving online which means that millions of citizens transfer their personal and biometric data to various digital systems on a daily basis.

In his annual address President of Kazakhstan Kassym Jomart Tokayev emphasized: "Based on large-scale digitalisation and the active implementation of artificial intelligence technology, we must modernise the economy". In response to this political course for 2024-2025, key legislative changes were initiated - ranging from the requirement for localization of personal data to the implementation of the Privacy by Design principle and the preparation of the draft law "On Artificial intelligence."[1]

On one hand this creates new opportunities for innovation and accelerates administrative and social processes. On the other hand it creates a number of risks to human rights related to data leaks, illegal processing or excessive collection. The purpose of my report today is to explain how Kazakhstan's personal data legislation has developed, what opportunities are opening up for the country in this area and what challenges and problems require urgent solutions and Artificial intelligence.

II. HISTORICAL DEVELOPMENT OF PERSONAL DATA REGULATION IN KAZAKHSTAN

After gaining independence, Kazakhstan began the formation of its own legal system, within which the protection of personal data gradually evolved into a constitutional principle of respect for private life. As noted by Zh.Ch Tegizbekova in her work "Through Law to Digital Security: Protection of Personal Data on Marketplaces in Central Asia" (in Digital Transformation: The Role of Artificial Intelligence and Big Data in Law, Governance and International Relations: Materials of the International Scientific and Practical Conference, Almaty,2025, pp.265-275), the development of legal regulation in this area reflects Kazakhstan's efforts to align national legislation with international standards of privacy protection. The Constitution of the Republic of Kazakhstan enshrines the right of every individual to privacy, personal and family secrets, and the protection of honor and dignity (Article 18), thereby establishing a constitutional foundation for data protection in the country.

Complementing this legal perspective, B. E.Abdrazak in "Storage and Processing of Data: Standardization and Infrastructure Requirements" (in Digital Transformation: The Role of Artificial Intelligence and Big Data in Law, Governance and International Relations: Materials of the International Scientific and Practical Conference, Almaty,2025,pp.54-61) highlights the importance of establishing unified technical standards and infrastructure requirements to ensure the security and integrity of information systems. The author emphasizes that the harmonization of data storage and processing mechanisms with international standards not only enhances cybersecurity but also supports the sustainable digital transformation of Kazakhstan's economy and governance systems.

A key milestone was the adoption of the Law of the Republic of Kazakhstan "On Personal Data and Their Protection" dated May 21, 2013, No. 94-V. [2] This document was the first systematic attempt to define what constitutes personal data, who the data subject is, what obligations the data operator bears, and what guarantees a citizen receives.

For the first time, concepts such as biometric data, personal data processing, personal data information systems were introduced, along with principles for their lawful processing.

Since 2013, the law has been changed multiple times. Between 2013 and 2025, the law was repeatedly supplemented: new articles were implemented (for example, Articles 8-1, 8-2), the powers of the supervisory authority were expanded, and provisions regarding cross-border data transfer, electronic resource security, and others were clarified.

The regulatory framework also gradually developed. In 2022, new Rules for the Collection and Processing of Personal Data (Order No. 102/NQ of the Ministry of Digital Development) were approved, along with requirements for data storage within Kazakhstan's territory.

The most significant reforms took place between 2023 and 2025. The changes concerned issues such as notification of personal data subjects, increased liability for data breaches, rules for cross-border data transfers, clarification of consent procedures, and data storage.

For example, as of July 1, 2024, operators are required to notify the Ministry of Digital Development, Innovations and Aerospace Industry about any personal data security breaches.[3] The collection and storage of paper copies of identity documents during personal data processing is prohibited. [3]

"Starting from 2025, key innovations in personal data regulation will come into effect in Kazakhstan. In particular, as of January 8, 2025, a mandatory localization requirement is introduced - databases containing personal data of citizens of the Republic of Kazakhstan must be stored on servers located within the country." [4]

"From January 8, 2025, mandatory localization of personal data of Kazakhstan citizens comes into force: databases stored in electronic information resources must be located on the territory of the Republic of Kazakhstan." [4] These changes aim to strengthen control and protection of citizens' data, as well as minimize leakage risks. The rules now include a new clause regarding the location of servers where personal data is stored. "Storage of personal data contained in electronic information resources shall be carried out by the owner and (or) operator, as well as by a third party, in an electronic database located in a server room or data processing center situated within the territory of the Republic of Kazakhstan, with necessary measures taken to protect personal data in accordance with these rules," the document states.

Additionally, on January 10, 2025, Law No. 155-VIII was signed, introducing amendments and additions to the Code of the Republic of Kazakhstan on Administrative Offenses. Changes were made to Article 79, significantly tightening administrative liability for violations of the personal data law: fines for individuals may reach up to 30 Monthly Calculation Indexes (MCI), and for businesses up to 200 MCI (depending on the scale). [5]

The MDDIAI order dated May 30, 2025, introduced clarifications to the Rules on integration with the state service for access control to personal data: precise definitions of terms such as "database operator," "security token," and "personal data subject" were introduced. [6]

Personal data subjects receive expanded rights: the right to delete, modify, block their data, the right to withdraw consent, and the right to know who and for what purpose processes their data. [7]

In May 2025, the MDDIAI order amended the rules on the integration of operators with government services for access to personal data: key terms,security token requirements,procedural aspects of integration, and protocols were clarified. [7]

These measures indicate that in 2025, personal data regulation in Kazakhstan is reaching a qualitatively new level - with enhanced control, liability, and territorial jurisdiction over databases.

III. NEW CHALLENGES OF DIGITAL IDENTITY

Special attention is deserved by the category of biometric data the most sensitive part of personal information. According to Article 1 of the Law of the Republic of Kazakhstan "On Personal Data and Their Protection," biometric data are defined as information characterizing the physiological and biological characteristics of a person on the basis of which their identity can be established.[2] These include facial images, fingerprints, iris patterns, voice, gait, and other unique parameters.

Starting from 2025, according to clause 2 of Article 12 of this law, new requirements for the protection and localization of such data are in force in Kazakhstan. [2]

1. Biometric data must be stored on servers located within the territory of the Republic of Kazakhstan.
2. Processing is allowed only with the written consent of the data subject, except for exceptional cases established by law (for example, for ensuring national security and law enforcement).

3. Transfer of biometric data abroad is only permitted if an equivalent level of protection is ensured in the recipient country (similar to the GDPR principle).

Today, biometrics are used in various digitalization areas:
1. for access to electronic government services (eGov),
2. in banking and financial services,
3. in video surveillance and security systems,
4. in mobile identification projects (Mobile ID),
5. in "Safe City" and "Digital Citizen Profile" systems.[8]

This increases the convenience and efficiency of digital services but simultaneously heightens risks - since biometric information is unique and immutable, its leakage can lead to lifelong vulnerability of the individual:
1. Leakage of biometric data is irreparable - unlike a password, a face or fingerprint cannot be "changed."
2. Informed consent is not always ensured - users are often unaware of who processes their data and for what purposes.
3. There is no unified supervisory authority for biometrics, although the creation of a specialized division under the Ministry of Digital Development of Kazakhstan is being discussed.
4. Projects on biometric monitoring and AI-based facial recognition are developing, which requires the implementation of ethical and legal safeguards to prevent mass surveillance without legal grounds.

In the context of the draft Law of the Republic of Kazakhstan "On Artificial Intelligence" (2025), it is proposed to:
1. establish mandatory principles for the ethical use of biometrics in AI systems;
2. implement Data Protection Impact Assessments (DPIA) when using facial recognition technologies;
3. prohibit automated decisions affecting human rights without human involvement in the final review.

Thus, biometrics is becoming a central topic in Kazakhstan's digital law: it demands a balance between innovation and personal protection, technical security, and legal accountability.

IV. CURRENT LEGISLATIVE INITIATIVES

In the Address to the People of Kazakhstan on September 2, 2025, President Kassym-Jomart Tokayev paid special attention to the development of artificial intelligence technologies, cybersecurity, and digital sovereignty.

The President emphasized that "the development of AI and digital solutions must take place in a safe and ethical environment, with reliable protection of citizens' data." [9] He particularly noted that the development of the digital economy is impossible without strengthening the legal guarantees of the individual and ensuring Kazakhstan's digital sovereignty, including data localization and transparency of operators' activities: "Based on extensive digitalization and active implementation of artificial intelligence technology, we must modernize the economy." This political message became a starting point for a set of regulatory initiatives and organizational measures aimed at creating a system of digital sovereignty and ensuring the security of personal data. [9]

In the 2024 Address to the People of Kazakhstan, President Kassym-Jomart Tokayev also outlined a new agenda for digital security. This directive became a key impetus for a series of legislative initiatives adopted in 2024–2025.

1. Amendments to the Law "On Personal Data and Their Protection" (2024–2025) - Key Changes:

A) Data Localization**.** In 2025, the requirement for localization was established: primary storage of databases containing personal data of citizens of the Republic of Kazakhstan must be carried out on servers located within the territory of Kazakhstan. This provision strengthens the territorial jurisdiction of the state over critical information infrastructure and is an element of digital sovereignty. (See subordinate acts and updated rules of the Ministry of Digital Development, 2025). [9]

B) Clarification of Consent and Notification Procedures. The amendments formalize the forms and procedures for obtaining consent (including electronic methods via eGov/Digital ID) and introduce an obligation for operators to notify the authorized body and the data subject of data breach incidents within specified timeframes. [3]

C) Privacy by Design. The law introduced a requirement to consider personal data protection at the design stage of digital services, including risk assessment and implementation of technical security measures. [2]

D) Administrative enforcement mechanisms against operators were strengthened (increased fines, expanded grounds for unscheduled inspections). These changes aim to improve compliance and minimize data breach risks. [2]

E) Cross-Border Transfer. For transferring personal data outside Kazakhstan, guarantees of equivalent protection in the recipient country and certification

mechanisms minimizing loss of control are required. [2]

2. Draft Law "On Artificial Intelligence" and Its Connection to Personal Data Protection

As part of the implementation of the "Digital Kazakhstan 2.0" program and by presidential mandate, the draft Law "On Artificial Intelligence" is being discussed in 2025, aimed at establishing legal and ethical AI standards.

Key provisions of the draft include:

1. Classification of AI systems by risk level (high- requiring strict control; medium and low - with proportionate requirements);
2. Establishment of principles for algorithmic transparency and explainability of decisions;
3. Introduction of mandatory Data Protection Impact Assessments (DPIA) when using AI technologies;
4. Direct prohibition of AI applications that violate human rights, including interference with privacy and discrimination;
5. Liability for developers and operators: establishing responsibility for harm caused by automated decisions and requiring "human oversight" in critical scenarios. [9]

Thus, Kazakhstan is moving toward the creation of a unified digital law system where personal protection becomes a cornerstone of innovative policy.

3. Administrative and Institutional Transformation

Within the digital strategy framework, the President instructed to accelerate the adoption of the Digital Code, strengthen state bodies, and consider the creation of a specialized authority (ministry/agency) on artificial intelligence and digital development. This indicates an intention to unify regulatory functions and create a centralized platform for coordinating policies in AI, data, and cybersecurity. [9]

The new changes aim to align national regulation with international practices (GDPR-like mechanisms, OECD AI recommendations). Academic and advisory centers play an important role, helping to develop national standards and train personnel. In particular, the School of Law and Public Administration (SLPA) of Narhoz University actively participates in governmental and research projects related to: personal data protection and digital rights of citizens, analysis of big data and AI regulation, and developing proposals for ethical oversight of digital technologies.

V. OPPORTUNITIES AND POSITIVE TRENDS

Despite ongoing challenges, Kazakhstan today demonstrates real advantages and positive shifts in the field of personal data protection and digital regulation.

1. Developed Digital Infrastructure

Kazakhstan remains the regional leader in digital transformation. Among the indicators characterizing Kazakhstan's digital readiness, note the following: 78th place in the Global Innovation Index 2024 (WIPO) [10], 24th position in the UN E-Government Development Index, and progress in the Global Cybersecurity Index (ITU) [11], where Kazakhstan is classified as Tier 2 with high ratings in legal and organizational measures.

1. UN E-Government Development Index (EGDI, UN): In the latest report, Kazakhstan rose to 24th place out of 193 countries on the e-government index (EGDI), reflecting a high level of digital provision of government services. [11]
2. Global Cybersecurity Index (ITU, GCI 2024): Kazakhstan demonstrated significant progress in GCI 2024 and was placed in Tier 2 (Advancing countries); the analysis showed a score of about 94.04/100 with high marks for legal and organizational measures. This indicates notable strengthening of national cyber and data infrastructure. [12]

Global Innovation Index (WIPO, 2024): Kazakhstan ranked 78th among 133 economies in GII 2024 (dated and method by WIPO). This gives an objective picture of the country's position in innovation and research potential. [10]

The established eGov platform and the implementation of electronic digital signatures have become the foundation for citizens' digital identity. Since 2024, eGov mobile services [13], biometric identification integration, and a unified digital profile have been actively developed. This creates a technological basis for safer and more personalized data processing.

2. Institutional Readiness and Legal Innovations

A significant institutional step in 2025 was the creation of the Ministry of Artificial Intelligence and Digital Development, based on the former Ministry of Digital Development, Innovations, and Aerospace Industry. The new ministry officially inherited rights and duties related to shaping state policy in digitalization, including functions for developing and coordinating personal data protection measures. This consolidation of functions (AI + data governance + cybersecurity) reflects the state's strategic approach: integrated management of digital transformation and data protection must ensure both digital sovereignty and citizen security. [14]

3. Security through Data: New Approaches to Crime Monitoring

Kazakhstan places special attention on protecting minors and preventing offenses involving them. Specialized geographic information system (GIS) maps display data on individuals prosecuted for

crimes against the sexual integrity of minors, as well as statistics on criminal offenses [23] committed by minors [24].

Such visualization allows identifying territorial trends, analyzing risk factors, and increasing the effectiveness of preventive measures. At the same time, the use of such maps requires strict adherence to confidentiality norms, personal data protection, and avoiding stigmatization of specific regions or social groups. These tools become an important element of digitalizing justice and social policy aimed at ensuring the safety and rights of childrenin Kazakhstan.

4. Potential for Harmonization with International Standards

Kazakhstan is steadily moving toward adapting the principles of GDPR (EU) and OECD standards. At the level of the EAEU, the possibility of developing a regional agreement on personal data protection is being discussed, which could strengthen trust in cross-border digital trade. [15]

Kazakh universities, government agencies, and international partners actively create platforms for experience exchange and joint research. Such collaboration promotes the formation of a safe, inclusive, and ethical digital ecosystem in Kazakhstan and Central Asia.

It is believed that Kazakhstan has a real opportunity to become a regional and international hub for data protection. To achieve this, it is necessary to consistently adapt national legislation to international standards (GDPR, OECD recommendations), participate in bilateral and multilateral agreements on cross-border data transfer, and formalize mechanisms for mutual recognition of certifications and protection standards. This course will not only enhance citizen rights protection but also create conditions for investment inflows and strengthen the country's digital sovereignty.

VI. CHALLENGES AND UNRESOLVED ISSUES

Despite positive shifts in regulation and institutional development, Kazakhstan still faces systemic problems that hinder the formation of a reliable, practice-oriented model for personal data protection.

1. The 2013 Law requires further adaptation to the realities of Big Data and AI

The Law "On Personal Data and Their Protection" was adopted in 2013; although amendments have been made, many provisions do not fully correspond to the realities of Big Data and AI (issues of automated processing, explainability, DPIA, etc.). Further detailing of concepts and responsibility mechanisms is needed. [2] The issue of cross-border data transfer remains open - when Kazakhstani personal data are stored in foreign clouds, jurisdiction and protection become unclear.

2. Social and Cultural Barriers

One of the toughest challenges for developing a culture of personal data protection in Kazakhstan remains the low level of digital and legal literacy among the population. Despite widespread technology adoption and high basic digital engagement, understanding of privacy principles and data protection remains limited.

According to the Statistics Committee of the Republic of Kazakhstan, digital literacy is steadily growing: if in 2018 the share of citizens with basic skills in device and online service use was 77.3%, by 2024 this would increase to 89.1% (age 6+) and 91.2% (age 6–74). The highest figures are in Astana (97.1%) and Almaty (96.9%), while some regions, e.g., North Kazakhstan (82.8%) and West Kazakhstan (85.2%), lag behind. [16]

Despite this progress, sociological studies (notably The Astana Times survey, 2024) show that understanding of data processing risks remains low. More than 60% of respondents admit giving consent to personal data processing without reading terms, and about 40% do not know how to check who and why uses their information. [17]

Practice shows that consent to data processing in Kazakhstan is often formal. Users habitually "click" consent without reading terms, especially when using biometric services such as face recognition, fingerprinting, and voice identification. Biometric data are unique and immutable, making leaks irreversible and potentially extremely dangerous. This requires stricter informed consent procedures and guarantees for data deletion or annulment upon withdrawal of permission.

As noted by the analytical portal CABAR.asia (2024), forming a data protection culture is impossible without active civic participation: people must not only have digital tools but also recognize the value of personal information as an intangible asset requiring responsible handling.

Thus, developing digital culture implies not only training technical skills but also raising legal awareness, trust, and user responsibility regarding their data. [18]

3. Supervisory Authority

International practice shows that effective oversight is ensured by independent Data Protection Authorities (DPAs), such as in France, Germany, or South Korea. In Kazakhstan, control over compliance with personal data protection rules is carried out by the Information Security Committee of the Ministry of Artificial Intelligence and Digital Development; that is, there is no agency with independence and authority comparable to European DPAs. This hinders systemic investigations, international cooperation, and development of consistent judicial practice. [19]

4. Algorithmic Opacity and Artificial Intelligence

Widespread use of surveillance systems, facial recognition, and algorithmic decision-making requires strict legal guarantees: auditability, purpose limitation, and appeal procedures. Without these, there is a substantial risk of unlawful monitoring and errors in algorithmic decisions. [20]

Even the AI draft law requires bylaws to specifically define who will be responsible for AI decision damages, how citizens can contest automated decisions, and how algorithm transparency is ensured. Without such mechanisms, automation risks leading to algorithmic discrimination, where decisions are made opaquely and without explanation.

5. Technical and Organizational Risks

In practice, most data breaches happen due to human factors rather than legal gaps. Often operators lack encryption, security audits, or basic access protocols. Small and medium businesses frequently do not conduct Privacy Impact Assessments. These gaps create serious cybersecurity risks.

The requirement to localize primary personal data storage in Kazakhstan improves control and digital sovereignty but creates technical and financial barriers for many operators.

The mandatory data localization starting 2025 is a significant demand. Many operators, especially SMEs, face technical, infrastructural, and financial hurdles: lack of server capacity, certification costs, security maintenance, regulatory adaptation. Compliance monitoring adds burden to supervisory bodies and requires new audit standards. [21]

6. Limited Judicial and Law Enforcement Practice

Despite the law, successful cases of protecting personal data rights are few. Though legislation is updated, there are few precedents where data subjects obtained real compensation or effective protection. This reduces deterrent effect and makes operator responsibility partly declarative. [22]

Kazakhstan consistently develops the regulatory framework, but real judicial and administrative enforcement cases remain rare. Notable cases include:

1. Case No.1: Bank “Bank RBK” (Decision of March 15, 2022, Nur-Sultan)

The specialized interdistrict court for administrative offenses found that JSC “Bank RBK” violated personal data laws, including:

- Failure to approve the list of personal data necessary for tasks;
- Failure to appoint a person responsible for organizing data processing;
- Failure to notify the authorized body about an information security incident.

A fine of 291,700 tenge was imposed under subparagraph 1, part 1, article 641 of the Code of Administrative Offenses of RK. (Based on materials from the Personal Data Protection Department, Information Security Committee, 2021–2022). [25]

2. Case No.2: JSC “Kazakhtelecom” (Decision of March 15, 2022)

Following an unscheduled inspection (Act No.30, May 18, 2021), the court found multiple violations, including:

- No person responsible for data protection;
- Non-compliance with data storage and transfer requirements with cryptographic protection;
- No identification means or processing event logs.

A fine of 204,190 tenge was imposed under the same article. (Based on citizen Shakenov A.A. 's complaint; investigation by the Personal Data Protection Department). [25]

Both rulings dated March 15, 2022, reflect inspections from 2021, showing that law enforcement is reactive and delayed (inspections → case initiation → court). Sanctions are administrative and mainly aimed at formally bringing documentation and procedures in order (appointing responsible persons, logs, cryptoprotection), not compensating data subjects.

The repeated violations - lack of appointed responsible persons, missing event logs, insufficient cryptoprotection indicate institutional and organizational weaknesses rather than isolated technical failures. These precedents suggest that state control is mainly formal: punishments address procedural violations but do not compensate for damage to citizens or build sustainable judicial practice.

7. Data Breaches in Kazakhstan: Timeline, Analysis, and Lessons

The years 2024–2025 can rightfully be called the most intense in the history of Kazakhstan’s cybersecurity. Widespread incidents of massive personal data leaks expose real weaknesses in infrastructure and law enforcement, as well as cast doubt on the ability of operators to comply with basic information security standards.

Timeline of high-profile incidents:

In summer 2025, a massive leak of about 16 million records from government databases occurred - including Individual Identification Numbers (IIN), contact details, and other information. This incident caused widespread public outcry and activated regulatory inspections. [26]

In May 2025, a Telegram bot was discovered that was distributing personal data of users and government employees, including publicly accessible information. The incident attracted media and regulator attention. [27]

In 2024–2025, leaks of client data from microfinance organizations (e.g., Zaimer.kz) were recorded, affecting millions of records - including contact data and IIN. [28]
In 2024, a special leak of more than 2 million microfinance sector client records was registered (according to media reports). In addition, official sources stated that more than 1.5 million operators, including government employees, banks, and services, had access to personal data. [29]
In 2023, damages from internet fraud (partially related to stolen data) exceeded 21 billion tenge, according to Kazakhstan's Ministry of InternalAffairs.[30]
In 2024–2025, leaks occurred in the healthcare and education sectors (regional cases of database compromises involving students, patients, and staff of universities and medical institutions). [31]
In 2025, large-scale global account database leaks also affected Kazakhstani users - emphasizing that national measures must be combined with global coordination.[32]

Analysis of the identified incidents shows the systemic nature of problems related to personal data protection in Kazakhstan. Almost in all cases of data breaches, there is insufficient protection of access channels, weak use of cryptographic mechanisms, absence of audit logs and monitoring, as well as ineffective control over third parties involved in data processing. It is notable that even large and technologically advanced operators commit elementary cybersecurity errors, indicating a formal approach to complying with legal requirements.

Despite the existence of a regulatory framework, including Personal Data Protection Rules and provisions of Article 641 of the Administrative Code of Kazakhstan [5], their practical compliance is often declarative. Data leaks demonstrate that many operators do not implement the required technical and organizational measures, do not conduct regular security audits, and fail to provide proper control over internal access procedures.
Particular concern arises from the fact that a significant portion of leaks involves citizens' identification information - primarily Individual Identification Numbers (IIN). Such information is especially valuable for criminals, increasing risks of phishing, social engineering, credit fraud, and illegal trafficking of personal data.
Large-scale incidents inevitably cause public outcry, increase media, civil society, and international expert attention, creating additional pressure on government bodies and operators. As a result, there is a tendency to strengthen control and supervisory measures and possibly revise standards of liability for violating data protection rules.
However, reactive measures - such as fines and violation recording are no longer sufficient. A shift from a punitive model to a preventive regulatory model is necessary, which should include:
- Mandatory Data Protection Impact Assessments (DPIA);
- Certification of operators and their security systems;
- Engagement of independent information security auditors;
- Mandatory incident reporting;
- Compensation mechanisms for citizens affected by data breaches.
Finally, data leaks should not be seen solely as a national problem. Global incidents show the interconnectedness of digital ecosystems: data compromise in one country often leads to chain reactions in another. Kazakhstan needs to take a more active role in international formats for sharing vulnerability information, standard unification, and joint response to cross-border cyber threats. Only such integration will strengthen citizens' trust and increase the resilience of the national personal data protection system.

VII. CONCLUSION AND RECOMMENDATIONS

Kazakhstan today stands on the threshold of a new digital era, where artificial intelligence, big data, and biometric technologies form the foundation of governance, economy, and public life. In this context, personal data protection goes beyond legal regulation - it becomes a key element of digital sovereignty, citizen trust, and ethical responsibility of the state and business.

Having modern legislation is an important but insufficient factor. It is crucial to ensure the real enforcement of norms, technological readiness of operators, and independence of oversight. Data leaks, growth in digital services, and development of AI systems require a systemic reform of risk management approaches and transparency in data processing.

Based on the above, the following practice-oriented recommendations can be highlighted:

1. It is advisable to consider creating a statutory independent data protection authority with powers for external investigations, enforcement orders, and its own budget. [19]
2. For all large digital projects - especially in biometrics and artificial intelligence - mandatory Data Protection Impact Assessments (DPIA) should be established with publication of summary reports on identified risks.
3. Support for small and medium enterprises during data localization. Implementation of requirements for data storage within Kazakhstan should be accompanied by government support measures for SMEs - including subsidizing data centers and certification of operators. [21]

4. Training judges, prosecutors, and investigators in digital and technological law is necessary, as well as creating fast-track cases for personal data protection and developing a base of precedents. [22]

Strategically, Kazakhstan needs to integrate norms on personal data, artificial intelligence, and cybersecurity into a unified Digital Code, establish biometric information protection standards, and ensure transparency of algorithmic decisions affecting citizens' rights.

Funding. The scientific article was prepared within the framework of funding for scientific and (or) scientific and technical programs for 2024-2026, aimed at the implementation of the IRN project AP23489796 "Problems of regulating the legal regime of big data: domestic and international experience", funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan."

BIBLIOGRAPHY

[1] Address of the President to the People of Kazakhstan – 2025. Zakon.kz News. Access:https://www.zakon.kz (accessed October 16, 2025).

[2] Law of the Republic of Kazakhstan No. 94-V of May 21, 2013 "On Personal Data and Their Protection." Access:https://online.zakon.kz/Document/?doc_id=31396226 (accessed October 16, 2025).

[3] Law of the Republic of Kazakhstan "On Amendments and Additions to Certain Legislative Acts of the Republic of Kazakhstan on Information Security, Informatization, and Digital Assets" No. 44-VIII ZRK of December 11, 2023. Access:https://adilet.zan.kz/rus/docs/Z2300000044 (accessed October 16, 2025).

[4] "Changes Introduced to the Rules for Implementing Personal Data Protection Measures by Owners, Operators, and Third Parties." Digital Rights Asia. Access:https://digitalrights.asia/events/servers-storing-kazakhstani-data-must-be-localized-in-kazakhstan-by-2025/ (accessed October 16, 2025).

[5] Code of the Republic of Kazakhstan on Administrative Offenses No. 235-V of July 5, 2014. Access:https://zakon.uchet.kz/rus/docs/K1400000235 (accessed October 16, 2025).

[6] "By Order of the MDDIAI Dated May 30, 2025, Amendments Were Made to the Rules for Integration with the State Service for Access Control to Personal Data." Zakon.kz.Access:https://www.zakon.kz/pravo/6480438-izmenilis-pravila-dostupa-k-personalnym-dannym.html (accessed October 16, 2025).

[7] Law of the Republic of Kazakhstan No. 94-V of May 21, 2013 "On Personal Data and Their Protection." Femida Justice Blog. Access:https://blog.femida-justice.com/aktualnye-voprosy-primeneniya-zakona-rk-o-personalnyh-dannyh-i-ih-zashhite-v-2025-godu-novye-trebovaniya-i-otvetstvennost/ (accessed October 16, 2025).

[8] E-Government of the Republic of Kazakhstan. Access:https://egov.kz/cms/ru (accessed October 16, 2025).

[9] "Digital Citizen Profile Will Appear in Kazakhstan." Inform.kz. Access:https://www.inform.kz/ru/tsifrovoy-profil-grazhdanina-poyavitsya-v-kazahstane-a8b6cd (accessed October 16, 2025).

[10] Official Address of the President of the Republic of Kazakhstan, September 2, 2025. Akorda.kz. Access:https://www.akorda.kz (accessed October 16, 2025).

[11] Global Innovation Index 2024. WIPO. Access:https://www.wipo.int/edocs/pubdocs/ru/wipo-pub-2000-2024-exec-ru-global-innovation-index-2024.pdf (accessed October 16, 2025).

[12] UN E-Government Development Index and Global Cybersecurity Index (ITU). Access:https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/87-Kazakhstan (accessed October 16, 2025).

[13] Global Cybersecurity Index (GCI 2024). ITU. Access:https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf (accessed October 16, 2025).

[14] E-Government Mobile Application "eGov Mobile." Access:https://egov.kz/cms/ru/information/mobile/mobile_application (accessed October 16, 2025).

[15] "Creation of the Ministry of Artificial Intelligence and Digital Development." The Astana Times, September 2025. Access:https://astanatimes.com/2025/09/kazakhstan-restructures-digital-ministry/ (accessed October 16, 2025).

[16] "Kazakhstan's Accession to the OECD Binding Legal Instrument." Bureau of National Statistics. Access:https://stat.gov.kz/ru/news/standarty-oesr-v-kazakhstane-prisoedinenie-kazakhstana-k-obyazatelnomu-pravovomu-instrumentu-oesr-re/ (accessed October 16, 2025).

[17] Bureau of National Statistics of the Agency for Strategic Planning and Reforms of the Republic of Kazakhstan. Access:https://stat.gov.kz (accessed October 16, 2025).

[18] Kazakhstan Reports High Digital Literacy and Internet Usage. The Astana Times, April 2025. Access:https://astanatimes.com/2025/04/kazakhstan-reports-high-digital-literacy-and-internet-usage/ (accessed October 16, 2025).

[19] Biometric Data Collection: What Risks Might Kazakhstanis Face? CABAR.asia. Access:https://cabar.asia/en/biometric-data-collection-what-risks-might-kazakhstanis-face (accessed October 16, 2025).

[20] DLA Piper Data Protection: Kazakhstan. Access:https://www.dlapiperdataprotection.com/index.html?c=KZ&t=law (accessed October 16, 2025).

[21] Orisbayev, Zholdas, and Reid Standish. "Kazakhstan Is Building a Surveillance State. Will China Be Its Model?" Radio Free Europe/Radio Liberty. Access:https://www.rferl.org/a/china-surveillance-hikvision-dahua-huawei-kazakhstan-ai-central-asia/33544093.html (accessed October 16, 2025).

[22] Kazakhstan Data Leak Exposes 16 Million IINs, Including Citizens from Russia, China, Uzbekistan & Kyrgyzstan. Digital Rights Asia. Access:https://digitalrights.asia/media/kazakhstan-data-breach-16-million-iin-russia-china-uzbekistan-kyrgyzstan/ (accessed October 16, 2025).

[23] Shyngyssov, Aset, and Bakhytzhan Kadyrov. Data Protection in Kazakhstan: Overview. Morgan Lewis LLP, 2023. Access:https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2023/data-protection-in-kazakhstan-overview.pdf (accessed October 16, 2025).

[24] ArcGIS Dashboard. "Map of Persons Prosecuted for Crimes Against the Sexual Inviolability of Minors." Committee on Legal Statistics and Special Records of the Prosecutor General's Office of the Republic of Kazakhstan. Access:https://gis.kgp.kz/arcgis/apps/dashboards/24a66201de214d20bafcc1e50c896b2a (accessed October 16, 2025).

[25] ArcGIS Dashboard. "Map of Criminal Offenses Committed by Minors." Committee on Legal Statistics and Special Records of the Prosecutor General's Office of the Republic of Kazakhstan. Access:https://gis.kgp.kz/arcgis/apps/dashboards/f775e72d0d6d4a9f8463a2e158e53a8c (accessed October 16, 2025).

[26] "Review of Court Practice on Bringing Kazakhstani Companies to Administrative Liability for Violating Personal Data Protection Requirements." Zakon.kz. Access:https://online.zakon.kz/Document/?doc_id=33158016 (accessed October 16, 2025).

[27] "The Ministry of Digital Development Commented on Reports of a Personal Data Leak Affecting Nearly All Kazakhstanis." Tengrinews.kz. Access:https://tengrinews.kz/kazakhstan_news/utechka-dannyih-16-millionov-kazahstantsev-mintsifryi-573113/ (accessed October 16, 2025).

[28] "Telegram Bot Found Distributing Personal Data of Users and Civil Servants." Kursiv Media. Access:https://kz.kursiv.media/2025-05-06/smrd-telegram-slivdannyh/ (accessed October 16, 2025).

[29] "In 2024–2025, Data Leaks of Microfinance Organizations' Clients (e.g., Zaimer.kz) Were Recorded." Azattyk Radiosy. Access: https://rus.azattyq.org/a/zhiteli-kazahstana-2024-krupneyshaya-v-istorii-kazahstana-dannye-bolee-16-millionov-kazahstantsev-utekli-v-set/33446017.html (accessed October 16, 2025).

[30] "Over Two Million Client Data Leaked from Microfinance Organizations in Kazakhstan: What Happened and What Are the Consequences?" Current Time TV. Access:https://www.currenttime.tv/a/32858487.html (accessed October 16, 2025).

[31] "Kazakhstanis Lost More Than 20 Billion Tenge to Internet Fraudsters in 2023." 24.kz. Access:https://24.kz/ru/news/social/681239-bolee-20-mlrd-tenge-poteryali-kazakhstantsy-iz-za-internet-moshennikov-v-2023-godu (accessed October 16, 2025).

[32] "In 2024–2025, Data Leaks in the Healthcare and Education Sectors Were Recorded." Inform.kz. Access:https://www.inform.kz/ru/utechka-dannih-16-mln-kazahstantsev-v-minzdrave-soobshili-o-proverke-po-faktu-intsidenta-b5ed6f (accessed October 16, 2025).

★★★