

Received: 28.06.2026. Accepted: 30.06.2026. Available online: 30.06.2026.

GRSTI 10.87.01

DOI: <https://www.doi.org/10.32523/2791-0954-2026-18-2-26-42>

**Personal data governance in the digital economies of Vietnam and Kazakhstan:
implementation challenges, cybersecurity risks and bilateral cooperation**

Marat Sarsembayev

Doctor of Law, Professor

Professor of the Department of International Law of L.N. Gumilyov ENU

Astana, Kazakhstan

e-mail: danecker@mail.ru

ORCID: 0000-0002-0340-8621

Trang Ly Hoang

Master of Law

Senior Specialist, International Cooperation Office, Hanoi Law University

Hanoi, Vietnam

email: hoangtrangly@gmail.com

ORCID: 0009-0008-1448-2027

Anh Thu Nguyen

Third year student

Department of Business Law of Hanoi Law University

Hanoi, Vietnam

e-mail: thunguyenanh005@gmail.com

ORCID: 0009-0004-3611-1762

Abstract. The article presents a comprehensive comparative analysis of the legal regulation of personal data in two developing countries – Vietnam and Kazakhstan. Both countries are demonstrating significant progress in the developing of e-commerce. Despite their success, they face a number of risks and challenges, especially in the field of legal regulation. The given article evaluates recent legislative initiatives aimed at building transparent e-commerce system and highlights some of the vulnerabilities that may be encountered in practice. To mitigate the issues discussed, the authors propose a number of solutions including in the field of mutual cooperation.

Keywords: personal data, digital economy, data governance, cybersecurity, legal regulation, Vietnam, Kazakhstan, bilateral cooperation

Вьетнам мен Қазақстанның цифрлық экономикаларындағы дербес деректерді реттеу: имплементация мәселелері, киберқауіпсіздік тәуекелдері және екіжақты ынтымақтастық

Сәрсембаев Марат Алдаңғорұлы

Заң ғылымдарының докторы, профессор

Л.Н. Гумилев атындағы ЕҰУ халықаралық құқық кафедрасының профессоры

Астана, Қазақстан

e-mail: daneker@mail.ru

ORCID: 0000-0002-0340-8621

Транг Ли Хоанг

Құқық магистрі

Ханой Заң университетінің халықаралық ынтымақтастық бөлімінің аға маманы

Ханой, Вьетнам

e-mail: hoangtrangly@gmail.com

ORCID: 0009-0008-1448-2027

Ан Тху Нгуен

Үшінші курс студенті

Ханой Заң университетінің кәсіпкерлік құқық кафедрасы

Ханой, Вьетнам

e-mail: thunguyenanh005@gmail.com

ORCID: 0009-0004-3611-1762

Андатпа. Мақалада екі дамушы ел – Вьетнам мен Қазақстандағы дербес деректерді құқықтық реттеудің жан-жақты салыстырмалы талдауы ұсынылған. Екі ел де электрондық коммерцияны дамытуда айтарлықтай прогреске қол жеткізді. Бұл жетістіктеріне қарамастан, аталмыш мемлекеттер бірқатар тәуекелдер мен қиындықтарға, әсіресе құқықтық реттеу саласындағы өзекті мәселелерге тап болды. Бұл мақалада екі елдегі электрондық коммерцияның ашық жүйесін құруға бағытталған соңғы заңнамалық бастамаларға баға беріледі және іс жүзінде кездесетін кейбір осалдықтар туралы айтылады. Мақалада талқыланған мәселелерді шешу мақсатында авторлар бірқатар ұсынымдар жасап, соның ішінде өзара ынтымақтастықты арттыру жолдарын саралайды.

Түйін сөздер: дербес деректер, цифрлық экономика, деректерді басқару, киберқауіпсіздік, құқықтық реттеу, Вьетнам, Қазақстан, екіжақты ынтымақтастық

Регулирование персональных данных в цифровых экономиках Вьетнама и Казахстана: проблемы имплементации, риски кибербезопасности и двустороннее сотрудничество

Сарсембаев Марат Алдангорович

Доктор юридических наук, профессор

Профессор кафедры международного права ЕНУ им. Л.Н. Гумилева

Астана, Казахстан

e-mail: daneker@mail.ru

ORCID: 0000-0002-0340-8621

Транг Ли Хоанг

Магистр права

Старший специалист отдела международного сотрудничества Ханойского

юридического университета

Ханой, Вьетнам

e-mail: hoangtrangly@gmail.com

ORCID: 0009-0008-1448-2027

Ань Тху Нгуен

Студент третьего курса

Факультет предпринимательского права Ханойского юридического

университета

Ханой, Вьетнам

e-mail: thunguyenanh005@gmail.com

ORCID: 0009-0004-3611-1762

Аннотация. В статье представлен всесторонний сравнительный анализ правового регулирования персональных данных в двух развивающихся странах – Вьетнаме и Казахстане. Обе страны демонстрируют значительный прогресс в развитии электронной коммерции. Несмотря на свои успехи, они сталкиваются с рядом рисков и вызовов, особенно в области правового регулирования. В данной статье дается оценка последних законодательных инициатив, направленных на построение прозрачной системы электронной коммерции, и освещаются некоторые уязвимости, с которыми можно столкнуться на практике. Чтобы смягчить остроту обсуждаемых проблем, авторы предлагают ряд решений, в том числе в области взаимного сотрудничества.

Ключевые слова: персональные данные, цифровая экономика, управление данными, кибербезопасность, правовое регулирование, Вьетнам, Казахстан, двустороннее сотрудничество

Introduction. It can be seen that the rapid development of the digital economy globally has turned personal data into an important production resource. In the world,

previous studies mainly focused on data protection under the GDPR standards or on legal analysis in each individual country, but no comprehensive research has specifically compared and deeply evaluated the personal data protection legal frameworks between Vietnam and Kazakhstan – two developing digital economies. This research gap creates a problematic situation, while opening opportunities for exploring the topic in a new context. The relevance of the topic is demonstrated by the theoretical and practical importance of personal data protection, as digital trust becomes a decisive factor for competitiveness, investment attraction and sustainable development in the digital economy.

Materials and methods. The study made extensive use of comparative legal analysis. The authors examined the laws of two countries, Vietnam and Kazakhstan, on personal data protection. They also conducted a comprehensive analysis of international treaties and other relevant documents. A quantitative approach was used to collect and analyze statistical data on data breach incidents.

Results and discussion. The article presents and critically discusses the main findings of the research concerning the protection of personal data subjects in the digital economy of Vietnam and Kazakhstan. Unlike previous studies that primarily focus either on the GDPR framework of European Union or on single-country legal analysis, this study adopts a comparative and interdisciplinary approach to examine two emerging digital economies that have received limited scholarly attention in the field of data governance.

Overview of personal data protection in the digital economy in Vietnam and Kazakhstan

Vietnam. Digital economy has emerged as a key driver of Vietnam's socio-economic development over the past decade. Supported by strong government commitment to digital transformation, Vietnam has witnessed rapid expansion across multiple digital sectors, including e-commerce, digital payments, fintech, digital platforms, and e-government services. According to VnExpress (2025a), In 2024, the digital economy grew at an estimated rate exceeding 20%, contributing approximately 18.3% of GDP and positioning Vietnam among the fastest-growing digital economies in Southeast Asia [1]. This growth has been supported by significant improvements in digital infrastructure and digital inclusion. Broadband connectivity, mobile internet coverage, and the gradual development of 5G networks have enhanced nationwide access to digital services. At the same time, the promotion of digital identity and digital public services has facilitated data integration across sectors such as healthcare, education, finance, and public administration, contributing to greater efficiency and service personalization.

In this context, personal data has become a central resource of the digital economy. Digital platforms, e-commerce operators, fintech companies, and state agencies increasingly rely on the collection, processing, and analysis of personal data to optimize services, enhance user experience, and support data-driven decision-making. Personal data thus plays a dual role: it is both an essential input for digital

economic growth and a subject of fundamental rights requiring effective legal protection.

However, the rapid expansion and increasing complexity of Vietnamese digital economy have also exposed significant challenges, creating growing pressure on existing legal, institutional and technical capacities, particularly with regard to personal data governance. First, the legal framework on personal data protection remains relatively new with gaps in implementation and enforcement, leading to legal uncertainty for digital service providers and limited effectiveness of safeguards for personal data subjects. Second, cybersecurity risks, data breaches, and digital fraud have increased, undermining trust in digital services as illustrated in Table 1.

Year	Total number of incidents	Online fraud	Data breaches	DDoS attacks
2022	11.200	5.600	3.100	2.500
2023	13.400	6.900	4.000	2.500
2024	15.800	8.200	5.100	2.500

Table 1. Statistics on Cybersecurity Incidents in Vietnam (2022–2024) [2]

Third, disparities in digital literacy and data protection awareness in Vietnam hinder individuals from effectively exercising their rights and managing personal data securely. According to research by Phan, Do, and Le, users' digital comprehension remains limited across multiple dimensions, despite over 42.62% demonstrating at least a basic level of understanding [3]. While respondents show relatively good awareness of personal data collection and use, significant gaps persist in policy-related knowledge, technical aspects, and data governance, with particularly low accuracy in understanding government policies. Overall, these challenges highlight that Vietnam's digital economy growth is accompanied by significant risks related to personal data governance. Addressing legal gaps, strengthening cybersecurity, and improving public awareness are therefore essential to ensure sustainable and trustworthy digital development.

For these reasons, Vietnam faces a pressing need to refine its legal and regulatory framework by learning from international experience. Comparative analysis of other developing digital economies, including Kazakhstan, can offer valuable insights into regulatory approaches, enforcement mechanisms, and pathways for harmonization with global standards.

Kazakhstan. The economy of the Republic of Kazakhstan has demonstrated significant growth in digitalization in recent years. This is clearly demonstrated by the development of the state e-government program, the emergence of large fintech companies such as *Kaspi* and *Freedom*, and the relocation of several well-known international IT companies to Kazakhstan. Major marketplaces such as *Wildberries*, *AliExpress*, and *Temu* have entered the Kazakhstan market, contributing to the overall growth of e-commerce.

The government is also making efforts to accelerate the digitalization of trade – the possibility of introducing electronic currency is being explored, and favorable legal conditions for the successful development of a digital business environment are being created. Significant developments included the adoption of the Law "On Digital Assets in the Republic of Kazakhstan" in 2023 and the "Digital Code" in early 2026. These legal acts have helped define a clearer framework for e-commerce.

Thanks to these efforts, the share of e-commerce in the domestic market in 2024 increased to 14.1% and now continues to grow. This figure is almost four times higher than in 2020.

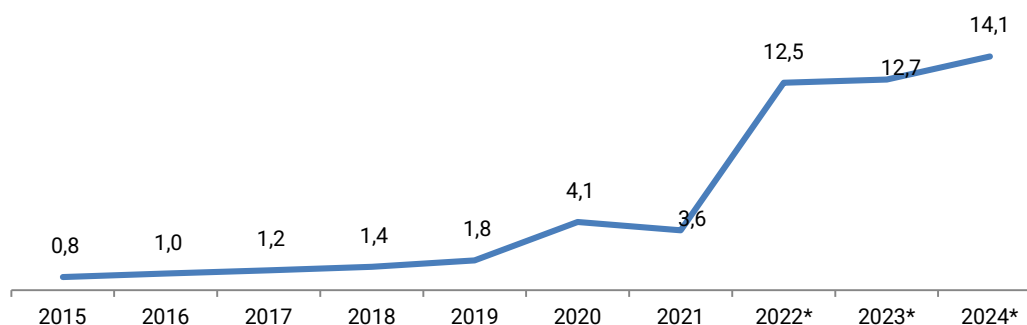


Diagram 1. The share of e-commerce in total retail trade in Kazakhstan [4]

In global rankings assessing the digital competitiveness of countries, Kazakhstan also performs well. However, over time, it has lost positions in some rankings, demonstrating the increasing level of digitalization worldwide [5]. In such a competitive environment, countries are encouraged to take more effective measures to develop the digital economy. In particular, policies aimed at increasing digital literacy and expanding broadband infrastructure should be a priority to maintain and accelerate economic growth [6].

Along with the rapid growth of the digital economy, the risk of crimes related to the leakage of personal data is unfortunately growing. One of the most pressing challenges of the current stage of digitalization has become the vulnerability of databases, leading to large-scale leaks of citizens' confidential personal information onto the global network. Compromises in the integrity and confidentiality of data not only undermine public trust in digital institutions but also create a fertile environment for the growth of cybercrime and financial fraud.

Statistics of information security incidents in recent years demonstrate alarming trends. A significant precedent was a series of major leaks recorded in 2024–2025. Specifically, in the spring of 2024, the databases of a large microfinance organization (zaimer.kz) became publicly accessible, affecting the personal data of over 2 million Kazakh citizens [7]. A similar leak occurred at several other microfinance organizations operating on the *Robo.finance* platform. The article notes that one of the companies affected by the leak was the Vietnamese microfinance organization «vietloan.vn». However, the most unprecedented incident was discovered later, when an archive with the working title "Residents of Kazakhstan 2024" was discovered online. This dataset, over 7 GB in size, contained over 16.3 million records, including

individual identification numbers, full names, residential addresses, and contact phone numbers [8]. Given the Kazakhstan's total population of approximately 20 million, this incident potentially affected the vast majority of the country's adult population.

The problem is exacerbated by the fact that many mobile operators collect excessive amounts of data without adequate cryptographic and organizational security measures. In response to these challenges, the government has initiated a number of protective mechanisms: a system for proactively notifying citizens about compromised data through the e-government portal (eGov) has been implemented, unscheduled inspections of businesses have been initiated, and penalties for the illegal circulation of personal information have been tightened. However, experience has shown that the existing personal data security architecture remains vulnerable to attackers and fraudsters. To comprehensively mitigate risks to Kazakhstan's digital economy, a large-scale transition to a preventative cybersecurity system is required, including legal mechanisms for protecting personal information, increasing digital literacy among the population, and toughening penalties for the illegal dissemination of personal data.

Common points in the impact of the digital economy on the need for personal data protection in both countries

The digital economies of Vietnam and Kazakhstan, while geographically distant, share striking similarities in how their rapid transformation has necessitated a fundamental shift in personal data protection. Both nations have transitioned from traditional economic models to data-driven ecosystems, where personal information has evolved from a private detail into a primary production resource.

The rapid expansion of the digital economy has fundamentally reshaped the regulatory landscape of personal data protection in both Vietnam and Kazakhstan, generating convergent pressures toward stronger legal safeguards while also exposing structural divergences rooted in governance models and regulatory maturity.

A significant common point is the dual role of personal data as both an economic catalyst and a vulnerability. In both countries, the rise of "super-apps" (such as *Zalo* in Vietnam or *Kaspi* Kazakhstan) and the expansion of E-government services have centralized vast amounts of citizen data. While this integration has significantly improved service personalization and administrative efficiency, it has simultaneously created prime targets for cybercriminals. Both nations have experienced large-scale data breaches, such as the 2024 leaks in Kazakhstan's microfinance sector and similar vulnerabilities in Vietnam's retail and fintech sectors [9], which have turned data protection from a technical preference into a matter of national security and public trust.

Furthermore, both Vietnam and Kazakhstan face a regulatory-technological gap. The pace of digital innovation in e-commerce, AI-driven credit scoring, and IoT-enabled smart cities has consistently outstripped the development of comprehensive legal frameworks. Consequently, both governments have recently moved toward codification as a solution. Vietnam's Law on Personal Data Protection (2025) and Kazakhstan's Digital Code (2026) both reflect a shared objective: to move away from

fragmented, sector-specific regulations toward a unified, modern standard that mirrors international benchmarks like the GDPR.

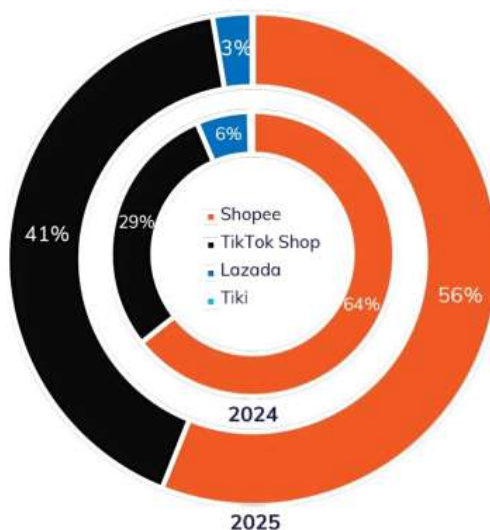
Lastly, there is a common societal challenge regarding digital literacy. In both countries, a large percentage of users demonstrate basic digital skills but lack deep awareness of data sovereignty, which is considered as the right to control how their information is harvested and traded by intermediaries. This disparity in awareness creates a lopsided ecosystem where digital platforms hold immense power over individual users. Therefore, in both Vietnam and Kazakhstan, the impact of the digital economy has made digital trust the decisive factor for future competitiveness. Both nations increasingly recognize that without a robust and transparent data governance regime, sustainable growth will be stifled by escalating cybersecurity threats and a deficit in public confidence.

It can be seen that the digital economy acts as both a catalyst for convergence and a source of divergence: while it compels both Vietnam and Kazakhstan to strengthen personal data protection regimes, it simultaneously accentuates differences in regulatory philosophy, institutional capacity, and the balance between economic openness and state control.

Practical implementation of the law on protecting the rights of personal data subjects in the digital economy in Vietnam and Kazakhstan

Vietnam. The practical implementation of legal provisions on protecting the rights of data subjects in Vietnam's digital economy can be observed through the privacy and security policies of corporations and companies, which reflect the level of compliance with legal requirements on personal data protection.

In the field of e-commerce, the privacy policy of Shopee can be taken as a representative example, as it currently holds a dominant market share in Vietnam.



Market share distribution of e-commerce platforms in Vietnam, 2024 – 2025 [10]

Shopee's privacy policy addresses three fundamental aspects of data processing, namely: what data is collected, when it is collected, and for what purposes it is processed. In other words, the company discloses the most basic elements of its data

processing activities, enabling users to gain a general understanding of how their personal data is handled. In addition, Shopee specifies certain circumstances under which the rights of data subjects may be restricted, as provided in Paragraph 7.3 of its policy. However, this company does not include a separate and explicit section on the rights of data subjects; instead, they are only indirectly reflected throughout the policy (for instance, Paragraph 13). Furthermore, Shopee has not publicly disclosed detailed procedures regarding data storage, data protection measures, or data processing impact assessments, particularly in cases involving cross-border data transfers or non-consensual processing. Notably, the provisions on cross-border data transfers in Paragraph 12 remain unclear, as they provide only minimal information. These limitations may increase the risk of insufficient transparency and undermine effective protection of data subjects' rights.

In the fintech sector, the policy on personal data protection and processing of the Joint Stock Commercial Bank for Investment and Development of Vietnam (BIDV) provides another illustrative example. In general, BIDV's policy is relatively comprehensive. It clearly identifies the entities involved in personal data processing (Paragraphs 1.6 to 1.9) and specifies the rights and obligations of data subjects in Paragraph 7.1.1. Moreover, the policy outlines the circumstances in which data subjects' rights may be restricted (Paragraphs 8.4 and 8.5), demonstrating compliance with current legal regulations. Importantly, the policy also describes a relatively complete personal data processing procedure in Paragraph 4, thereby enabling users to better understand how their data is handled [11]. However, the most recent update of this policy dates back to 2024, whereas the Law on Personal Data Protection has come into force in 2026. This indicates that, despite its relative completeness, the policy has not yet incorporated several new legal requirements. For example, it does not specify the obligation to notify competent authorities and data subjects in the event of personal data breaches, as required under Article 27(1) of the Law on Personal Data Protection and Article 8(3) of Decree No. 356/2025/ND-CP. In addition, the policy does not clearly define the information that must be provided to users when obtaining their consent for data processing. These shortcomings suggest the need for further revision and improvement in the future.

In conclusion, although corporate privacy policies in Vietnam have reached a certain level of completeness, they have not yet fully incorporated the latest legal requirements. Moreover, as the law does not mandate full public disclosure of all data processing procedures, there remains a risk of insufficient transparency in personal data processing activities.

Difficulties and requirements for improving the law on protecting the rights of personal data subjects in the digital economy in Vietnam.

From a legal perspective, Article 19(2) of the Law on Personal Data Protection grants enterprises the autonomy to establish their own internal monitoring mechanisms for personal data processing. However, this provision does not set out specific criteria regarding the content, standards, or operational procedures of such mechanisms, nor does it impose any obligation of public disclosure. As a result, enterprises are free to

design these mechanisms at their discretion, leading to inconsistencies in implementation and difficulties in assessing compliance. In the context of the digital economy, where data processing activities are complex, large-scale, and often cross-border, the lack of transparency places data subjects in a passive position. They are not provided with sufficient information to effectively monitor how their data is handled or to exercise their rights, such as the right to be informed, the right of access, or the right to object to data processing.

From practical perspective, as previously discussed, many enterprises have not proactively disclosed their data processing impact assessment (DPIA) mechanisms or the specific data protection measures tailored to their services. In addition, the delayed incorporation of newly enacted legal provisions into corporate policies highlights a gap between the legal framework and its practical implementation. This gap has direct implications for data subjects: they are unable to assess the level of protection afforded to their personal data, remain unaware of the scope and purposes of data processing, and may encounter obstacles when attempting to exercise their legal rights. In the long term, such limitations not only undermine the effectiveness of personal data protection but also erode user trust in digital platforms, an essential foundation of the digital economy.

In response to these challenges, the government has initiated several measures to enhance the effectiveness of legal enforcement. These include organizing specialized training programs and professional development activities on personal data protection for enterprises and relevant stakeholders. At the same time, efforts have been made to develop guidance materials, promote legal awareness, and strengthen public communication [12]. These initiatives aim to bridge the gap between legal provisions and practical implementation, thereby improving the protection of data subjects' rights in the digital environment.

Kazakhstan. The primary law in the field of personal data protection in Kazakhstan is the Law of the Republic of Kazakhstan dated May 21, 2013, "On Personal Data and Its Protection." This law defines the concept of "personal data protection." According to paragraph 11 of Article 1 of the law, personal data protection is a set of measures, including legal, organizational, and technical ones, implemented for the purposes established by this law [13].

For ease of understanding by the reader, the personal data protection measures provided for in the Law can be divided into several categories:

The first category is technical and organizational requirements. Article 22 sets forth the obligations of the owner or operator, who must take all measures to: 1) prevent unauthorized access to personal data; 2) promptly detect instances of unauthorized access to personal data if such unauthorized access could not be prevented; 3) minimize the adverse consequences of unauthorized access to personal data; 4) provide the state technical service with access to information technology facilities to conduct security assessments of the storage, processing, and dissemination of restricted personal data; 5) register and maintain records of the above actions.

Secondly, the law (Article 12) requires the storage of personal data by the owner and operator, as well as by a third party, in a database located in the Republic of Kazakhstan.

The next category of measures is aimed at promptly informing both citizens and the authorized body about leaks and potential risks.

It is also important to note that the law defines the conditions under which and according to the legal principles that personal data must be collected. For example, according to Article 7 of the Law, the collection and processing of personal data must be limited to achieving specific, predetermined, and legitimate purposes, and if the content and volume of information is excessive in relation to the purposes of its processing, this will constitute a violation. Article 8 regulates the procedure for granting (or revoking) a subject's consent to the collection and processing of personal data.

Finally, the state must play a central role in all of this, acting as a regulator. The authorized body is empowered to conduct periodic and unscheduled inspections of businesses and government agencies to ensure compliance with cybersecurity requirements and data processing rules. Failure to comply with these requirements entails strict administrative and, in severe cases, criminal liability.

The Law of the Republic of Kazakhstan dated November 24, 2015, "On Informatization" largely replicates the content of the Law "On Personal Data" in terms of ensuring the security of personal data, although the law itself is aimed at regulating public relations in the field of informatization. The law stipulates the terms of information use for the development of ICT, e-government, and other tools that facilitate the growth of automation and digitalization in the country. Unlike the first law, it addresses not only the protection of personal data but also the country's cybersecurity as a whole. Some believe that this law will soon be transformed into the Law "On Cybersecurity" [14].

The adoption of the Digital Code in early 2026 marked another step toward the digitalization of public relations in the country. The Code contains a number of articles regulating the use of personal data. For example, according to Article 41, citizens of Kazakhstan have the right to delete, anonymize, and limit the processing of their personal data [15].

Along with the rights and obligations of personal data subjects, it is worth paying attention to the issue of liability for violating Kazakhstan's legislation on personal data protection. According to Article 79 of the Code of the Republic of Kazakhstan "On Administrative Infractions", the following violations of the law on personal data protection are established (if the act does not constitute a crime):

- 1) illegal collection and/or processing of personal data committed by the owner, operator, or third party using their official position;
- 2) failure by the owner, operator, or third party to comply with measures to protect personal data;

may entail fines ranging from 20 to 1,000 MCI (Monthly Calculation Index), depending on the category of the business entity and the qualifying elements of the administrative offense.

Article 211 of the Criminal Code of the Republic of Kazakhstan provides for criminal penalties for the unauthorized distribution of electronic information resources containing citizens' personal data or other information, access to which is restricted by the laws of the Republic of Kazakhstan or by their owner or possessor. Penalties, depending on the severity of the offense, include: a fine of 200 MCI; correctional labor; community service for up to 1,200 hours; arrest for up to 15 days; deprivation of the right to hold certain positions or engage in certain activities for up to five years; restriction of freedom for up to five years; and imprisonment for up to seven years [16].

Overall, Kazakhstan's economy is confidently moving toward digitalization. Legislators are striving to keep pace with technological progress. Laws adopted in recent years demonstrate Kazakhstan's readiness for fundamental changes aimed at developing the digital economy.

Kazakhstan, in our opinion, should become a party to the Convention No. 108 on the Protection of Personal Data of January 1, 1985, as well as Protocol No. 223 of October 10, 2018. Thus, we would gain additional international experience in the protection and protection of personal data of citizens of the Republic of Kazakhstan. We need this because personal data often becomes public, despite the lack of consent from Kazakhstani citizens. Cybercriminals use these circumstances to commit seizures of billions of dollars of citizens of the republic. Penalties for cybercrimes should be tightened. It seems that the judicial proceedings in every criminal case involving cybercriminals should be public: thus, the citizens of the country will massively learn how to resist the fraudulent actions of cybercriminals, they will know in advance how to prevent these scammers from accessing their codes, personal data, no matter what tricks they may resort to.

It makes sense that it would be desirable to develop and adopt a similar Convention on the protection of personal Data within the CIS, which would also strengthen the cybersecurity of citizens of our region, including the Republic of Kazakhstan. Such a Convention can be adopted on the basis of the model law "On Personal Data", which was approved by a resolution at the 14th plenary session of the Interparliamentary Assembly of the CIS Member States on October 16, 1999, in which the term "personal data" means information about a person posted on a tangible medium that is reliably identified with a specific person." [17].

Resolutions of a recommendatory nature on personal data issues are being adopted at the UN level, for example, UN General Assembly Resolution No. 73/179 of December 17, 2018 "The right to privacy in the digital age" was adopted <https://undocs.org/ru/A/RES/73/179> (date of access: 04/21/2026). But such documents are binding. Therefore, it is necessary to adopt an appropriate Convention on these issues at the UN level and under the auspices of the United Nations. Kazakhstan could act as the initiator of the development and adoption of a universal multilateral convention on the protection of personal data of citizens. In this regard, it would be

advisable to use and expand the provisions of article 36 of the UN Convention against Cybercrime, European international legal acts on personal data in order to develop a separate international-legal act aimed at protecting personal data on a global scale. Such a convention is also necessary because cyber-attacks on confidential data of government organizations and business institutions, as well as citizens, have become more frequent in recent years [18, p. 28].

Legal Challenges in Bilateral Digital Economic Cooperation

Although Vietnam and Kazakhstan have made substantial progress in developing their digital economies, several legal challenges continue to hinder deeper bilateral digital economic cooperation.

First, differences in legal terminology, regulatory approaches, and compliance requirements create legal uncertainty for enterprises operating across jurisdictions. Variations in consent procedures, cross-border data transfer requirements, and data localization obligations increase compliance costs and administrative burdens for businesses engaged in digital trade, e-commerce, and fintech activities.

Second, both countries lack a bilateral legal framework specifically governing cross-border data governance and mutual recognition of personal data protection standards. The absence of interoperable legal mechanisms complicates international data transfers and reduces legal certainty for digital service providers.

Third, enforcement challenges remain significant in the digital environment. Personal data violations frequently involve cross-border digital activities that exceed the territorial jurisdiction of national authorities. In practice, limitations relating to evidence collection, international cooperation, and the recognition of foreign enforcement measures reduce the effectiveness of legal protection for personal data subjects.

Another challenge concerns digital literacy and public awareness. Many individuals remain insufficiently informed about their rights relating to personal data protection, thereby limiting their ability to effectively monitor and control how their information is collected, processed, and transferred in the digital economy.

Finally, tensions between national sovereignty and the free flow of information continue to influence the regulatory policies of both countries. While Vietnam places stronger emphasis on state supervision and data localization, Kazakhstan demonstrates relatively greater openness toward international digital integration. These differences may complicate efforts to establish harmonized legal standards for bilateral digital cooperation.

Proposed Legal harmonization solutions between the two countries

To strengthen personal data protection and promote sustainable digital economic cooperation, Vietnam and Kazakhstan should gradually harmonize their legal frameworks in accordance with international standards and practical digital governance needs.

First, the two countries should establish bilateral cooperation mechanisms relating to cybersecurity and personal data governance. Such mechanisms may include

information-sharing systems, joint policy dialogues, and mutual legal assistance in investigating cross-border data violations and cybercrime.

Second, both countries should develop interoperable legal standards governing cross-border data transfers. In particular, clearer and more transparent rules concerning consent, data processing obligations, breach notification, and accountability mechanisms should be introduced to reduce legal uncertainty for businesses and individuals.

Third, Vietnam and Kazakhstan should strengthen institutional capacity and enforcement effectiveness through specialized supervisory authorities, professional training programs, and clearer compliance guidance for enterprises operating in the digital economy.

Fourth, legal harmonization efforts should prioritize internationally recognized principles such as accountability, transparency, proportionality, and data security. Aligning domestic legislation more closely with frameworks such as the GDPR, OECD Privacy Guidelines, and APEC Privacy Framework would facilitate digital trade while ensuring adequate protection for personal data subjects.

Finally, both countries should promote digital literacy and public awareness programs in order to improve understanding of personal data rights and strengthen digital trust among citizens and businesses.

Recommendations for Applying International Standards and Data Protection Mechanisms in the Digital Economy

Vietnam and Kazakhstan should continue modernizing their personal data protection regimes in line with international best practices while adapting them to domestic socio-economic conditions.

First, greater emphasis should be placed on accountability mechanisms. Enterprises processing personal data should not only comply with legal obligations but also demonstrate compliance through internal monitoring systems, transparent policies, and data processing impact assessments.

Second, transparency obligations should be strengthened in sectors involving large-scale personal data processing, particularly e-commerce, fintech, digital advertising, and online platforms. Individuals should be clearly informed about the scope, purpose, duration, and risks of data processing activities.

Third, cross-border data transfer mechanisms should be improved through contractual safeguards, certification systems, and international cooperation frameworks aimed at facilitating secure digital trade and data governance interoperability.

Fourth, governments should enhance enforcement effectiveness by increasing administrative and criminal sanctions for serious violations, strengthening cybersecurity systems, and improving international cooperation against cybercrime and unlawful exploitation of personal data.

Finally, both countries should invest in long-term digital literacy programs, cybersecurity education, and professional capacity-building in order to create a sustainable and trustworthy digital environment.

Conclusion. The findings of this study have important implications for both legal policy and digital economic governance. Strengthening personal data protection is essential not only for safeguarding privacy rights but also for maintaining public trust, promoting innovation, and ensuring sustainable digital economic growth.

For Vietnam and Kazakhstan, closer legal harmonization and stronger international cooperation in personal data governance would facilitate cross-border digital trade, improve legal certainty for businesses, and enhance the effectiveness of cybersecurity and privacy protection mechanisms.

More broadly, the study demonstrates that personal data protection in emerging digital economies should not be viewed solely as a privacy issue, but also as a matter of digital sovereignty, economic competitiveness, and transnational governance in the digital era. Effective and transparent data governance frameworks will therefore play an increasingly important role in shaping the future of bilateral digital economic cooperation between Vietnam and Kazakhstan.

References.

1. Anh, N.. (2025a4). 'Digital economy contributed 18.3% to GDP', VnEconomy, URL: <https://en.vneconomy.vn/digital-economy-contributed-18-3-to-gdp.htm> (date of access: 28 June 2026)
2. Huỳnh, P.D. and Nguyễn, P.L. (2025) 'Bảo mật thông tin – Nền tảng phát triển kinh tế số bền vững tại Việt Nam' [Information security – The foundation for sustainable digital economic development in Vietnam], *Chuyên trang Nghiên cứu Kinh tế - Tài chính*. URL: <https://nghienccuu.tapchikinhhtetaichinh.vn/bao-mat-thong-tin-nen-tang-phat-trien-kinh-te-so-ben-vung-tai-viet-nam-104372.html> (date of access: 28 June 2026)
3. Phan B.T, Do P.H, Le D.Q. (2025). "The Impact Of Digital Literacy On Personal Information Security: Evidence From Vietnam". In Proceedings of the International Conference on Emerging Challenges: Sustainable Strategies in the Data-driven Economy (ICECH 2024). Atlantis Press. https://doi.org/10.2991/978-94-6463-694-9_32. (date of access: 28 June 2026)
4. The share of e-commerce in total retail trade // The official website of the Bureau of Statistics of the Republic of Kazakhstan URL: [https://stat.gov.kz/upload/iblock/f07/fnza05wfy2mpjls1lqk75dqt7wyfa3du/%D0%91-07-05-%D0%93%20\(2024\)%20%D1%80%D1%83%D1%81.pdf](https://stat.gov.kz/upload/iblock/f07/fnza05wfy2mpjls1lqk75dqt7wyfa3du/%D0%91-07-05-%D0%93%20(2024)%20%D1%80%D1%83%D1%81.pdf) (date of access: 28 June 2026)
5. Buganova A.A., Umirzakov S.Y., Nurpeisova A.A. DIGITAL ECONOMY AND DIGITAL TRANSFORMATION IN KAZAKHSTAN. Central Asian Economic Review. 2022;(5):155-168. (In Russ.) URL: <https://doi.org/10.52821/2789-4401-2022-5-155-168> (date of access: 28 June 2026)
6. Kalybekova D.B., Yeszhanova Zh.Zh. Trends in the development of the digital economy in Kazakhstan: statistical analysis. Central Asian Economic Review. 2025;(4):264-277. URL: <https://doi.org/10.52821/2789-4401-2025-4-264-277> (date of access: 28 June 2026)

7. Утечка данных: что делать казахстанцам, получившим уведомление от zaimer.kz // Сетевое издание "zakon.kz" URL: <https://www.zakon.kz/obshestvo/6427086-utechka-dannykh-chto-delat-kazakhstantsam-poluchivshim-uvedomlenie-ot-zaimer.kz.html> (date of access: 28 June 2026)
8. В Минцифры сделали заявление по "утечке данных более 16 млн казахстанцев // Сетевое издание "zakon.kz" URL: <https://www.zakon.kz/obshestvo/6481146-v-mintsifry-sdelali-zayavlenie-po-utechke-dannykh-bolee-16-mln-kazakhstantsev.html> (date of access: 28 June 2026)
9. Công an Nhân dân (2025)., ‘VNCERT khuyến cáo người dân nâng cao cảnh giác sau sự cố lộ dữ liệu tín dụng’ [VNCERT advises people to be more vigilant after credit data leak incident]. URL: <https://cand.com.vn/Cong-nghe/vncert-khuyen-cao-nguoi-dan-nang-cao-canhh-giac-sau-su-co-lo-du-lieu-tin-dung-i781095/> (date of access: 28 June 2026)
10. VnExpress (2026)., “Shopee, TikTok Shop chiếm 8% thị phần ngành bán lẻ,”. URL: <https://vnexpress.net/shopee-tiktok-shop-chiem-8-thi-phan-nganh-ban-le-5005886.html>, (date of access: 28 June 2026)
11. BIDV (2024)., “Phụ lục – Điều khoản và Điều kiện chung của BIDV về Bảo vệ và xử lý dữ liệu cá nhân”,. URL: <https://bidv.com.vn/wps/wcm/connect/5c9044ca-15b4-42c1-ae93-24cb3ba8fbb8/%C4%90K%C4%90K+chung+v%E1%BB%81+b%E1%BA%A3o+v%E1%BB%87+d%E1%BB%AF+li%E1%BB%87u+c%C3%A1+nh%C3%A2n.pdf?MOD=AJPERES&CVID=oVW8ktS> (date of access: 28 June 2026)
12. Section II.3 of Decision No. 2623/QĐ-TTg (2025) on the Plan for the Implementation of the Law on Personal Data Protection (date of access: 28 June 2026)
13. On Personal Data and their Protection // Legal information system of Regulatory acts of the Republic of Kazakhstan “Әділет”. URL: <https://adilet.zan.kz/eng/docs/Z1300000094/compare> (date of access: 28 June 2026)
14. Закон о кибербезопасности появится в Казахстане // URL: <https://uchet.kz/news/zakon-o-kiberbezopasnosti-poyavitsya-v-kazakhstane/> (date of access: 28 June 2026)
15. Digital Code of the Republic of Kazakhstan // Legal information system of Regulatory acts of the Republic of Kazakhstan “Әділет”. URL: <https://adilet.zan.kz/rus/docs/K2600000255> (date of access: 28 June 2026)
16. Penal Code of the Republic of Kazakhstan // Legal information system of Regulatory acts of the Republic of Kazakhstan “Әділет”. URL: <https://adilet.zan.kz/eng/docs/K1400000226> (date of access: 28 June 2026)
17. Model section "On personal tribute" (Article 2) // Information Bulletin of the Interparliamentary Assembly of the CIS. 2000. № 23 - <https://base.garant.ru/2569222/741609f9002bd54a24e5c49cb5af953b/> (date of access: 28 June 2026)
18. Saidmukhtorov A.A. Cyberspace as a new type of space in international law // Eurasian Journal of International Law. 2024. No. 3 (11). Pp. 23-36.

Authors' contributions

The article was written by authors from Kazakhstan and Vietnam.

1) Marat Sarsembayev analyzed Kazakhstani legislation, reviewed international documents on personal data protection, and proposed measures to improve Kazakhstani legislation.

2) Trang Ly Hoang analyzed Vietnamese legislation, developed the research methodology, and put forward proposals to improve the harmonization of the two jurisdictions.

3) Anh Thu Nguyen reviewed and compiled the statistical data presented in the work and analyzed Vietnamese legislation for compliance with international standards.