SCIENCEZONE | ONLINE SCIENTIFIC CONFERENCES

LEGAL ASPECTS OF CYBER SECURITY AND DATA PROTECTION IN THE FIELD OF FINANCIAL TECHNOLOGIES: INTERNATIONAL AND NATIONAL EXPERIENCE

Temurbek Polatov

Lectuer of Cyber Law Department, Tashkent State University of Law

p.001@gmail.com

Abstract: The article provides a comprehensive analysis of the current state of cyber security and data protection in the field of financial technology (fintech). The research covers a wide range of topics, from analyzing current cyber threats to examining international legal standards, including a detailed review of the GDPR and national regulatory requirements of various jurisdictions. Particular attention is paid to the experience of the Republic of Uzbekistan in creating an effective system of cyber security regulation in the field of fintech. Based on the research, practical recommendations were developed to implement complex data protection measures and ensure compliance with the requirements of regulatory documents. Innovative approaches to improving the legal regulation of cyber security in the fintech sector are proposed, taking into account the specific characteristics of developing markets and the global trends of digitalization of the financial sector.

Keywords: financial technology, cyber security, data protection, GDPR, legal regulation, fintech, digital economy, information security, personal data, international standards, financial sector, banking system, digital transformation

Introduction

The current era of digital transformation of the financial sector is characterized by the unprecedented growth of financial technologies that are fundamentally changing traditional approaches to the provision of financial services. According to the results of international studies , the global market of fintech services has an annual growth rate of 23.4 percent, which creates new challenges for cyber security and data protection systems.

A positive study of technology for 2023 shows an alarming trend: the number of cyberattacks on the financial sector has increased by 20% compared to the previous period, with 67% of attacks targeting fintech companies. In Uzbekistan, according to the report of the Central Bank, the situation is also alarming: in 2023, more than 1,000 attempts to gain unauthorized access to banking systems were recorded, which is 35% more than in 2022.

In the fundamental study of SS "Digital" economy: molyavium technological and cyber security, professor SS Gulomov states that the development of the digital economy requires the creation of a complex system of financial information protection, taking into account both technological and legal aspects of security. This issue is related to financial systems and financial the integration of systems is particularly relevant in the context of the increase in the volume of cross-border financial transactions .

In the conditions of Uzbekistan, where digitalization of the financial sector is being carried out especially rapidly, cyber security issues are gaining strategic importance. According to the information of the Central Bank of the Republic of Uzbekistan, the number of users of digital financial services has increased by 45% in the last year in our country, creating additional risks for the security of the financial system .

2. Cyber threats in fintech

2.1 Classification of modern threats

The modern landscape of cyber threats in the Fintech sector is characterized by high dynamism and constant evolution of attack methods. Abdullaev MK "Uzbekistan" in the research "fintech security: theory and practice" deeply

analyzes modern cyberthreats and highlights their main categories and characteristics .

Targeted attacks on payment systems pose the most serious threat to the fintech sector. Attackers use advanced techniques to bypass security systems, including exploiting zero-day vulnerabilities and using artificial intelligence to automate attacks. In 2023, more than 200 attempts to break into payment systems were recorded in Uzbekistan, 15% of which can be classified as high-tech attacks.

Hacking users' personal data is becoming an increasingly serious problem. In the era of digital finance, personal information has become a valuable asset for cybercriminals. According to NGKarimov's research, in 2023, more than 500 cases related to the leakage of personal data of users of fintech services were recorded in Uzbekistan .

Social engineering fraud is becoming increasingly sophisticated. Criminals are actively using deep learning techniques to create credible phishing campaigns and fake financial applications. Financial losses from social engineering in Uzbekistan in 2023 amounted to more than 12 billion soums.

2.2 The impact of cyber threats on the financial sector

The impact of cyber threats on the financial sector is complex and affects various aspects of financial institutions' operations. Studies of Karimov NG. It shows that the average loss from a single cyber security incident in Uzbekistan's banking sector is about US$50,000, with indirect losses likely to be much higher.

Reputational risks are becoming an increasingly important factor. According to a study conducted by Tursunov BO, more than 60% of customers are ready to abandon the services of a fintech company after a serious security incident. This puts additional pressure on companies to ensure that data and systems are reliably protected .

3. International legal standards of data protection

3.1 GDPR as a reference standard

The General Data Protection Regulation (GDPR) has significantly changed the global data protection landscape by setting new standards for the processing of

personal data. The principle of data minimization enshrined in the GDPR requires fintech companies to collect and store only the data that is truly necessary for the provision of services. This significantly reduces the risk of data leakage and unauthorized use .

The right to data portability has become an important means of ensuring competition in the fintech sector. Users have the opportunity to freely transfer their data between different services, which helps to develop the market and improve the quality of services. Fintech companies must provide the technical capabilities of such a transfer, which requires additional investment in infrastructure.

Mandatory 72-hour breach reporting has become the industry standard for transparency. The Data Protection Officer plays a key role in ensuring GDPR compliance by coordinating all aspects of data protection within the organization. Regularly conducting data protection impact assessments allows timely identification and elimination of potential risks.

3.2 Implementation of international standards

The process of harmonization of national legislation with international standards is particularly active in Uzbekistan. The Law "On Personal Data" No. O'RQ-547 largely complies with the principles of the GDPR, which sets high standards for the protection of personal data. Particular attention is paid to ensuring the rights of data subjects and defining the specific obligations of personal data operators.

The Central Bank of Uzbekistan has developed a set of regulatory documents regulating information security issues in the financial sector. These documents take into account the international experience and adapt it to the specific characteristics of the national market. Special attention is paid to cross-border data transfer and security in the use of cloud technologies.

4. National legal norms

4.1 Features of national regulation

The cybersecurity regulatory framework in fintech is a multi-tiered structure based on interrelated legislation. The main document is the Law No. ORQ-547 "On Personal Data", which defines the basic principles of personal data

processing and requirements for their protection. A particularly important aspect of this law is the definition of categories of personal data and the establishment of special requirements for the processing of biometric data, which are very important for the fintech sector in the context of the development of biometric identification .

The new version of the Law "On Electronic Commerce" significantly expanded the requirements for the security of electronic payments and the protection of user data during financial transactions. As Shermuhamedov AT noted in his research, this law created a legal basis for the introduction of innovative fintech solutions while ensuring a high level of security.

According to Presidential Decree No. PQ-4022 "On additional measures for the development and implementation of the digital economy", strategic priorities in the field of digitization of the financial sector were determined and the main directions for the development of cyber security systems were determined. . The document envisages the creation of a national cyber security system and defines the mechanisms of mutual cooperation of state bodies and the private sector in the field of information security.

The Central Bank of Uzbekistan has developed a set of regulatory legal documents regulating information security issues in the banking sector. The regulation "On requirements for ensuring information and cyber security in the implementation of bank operations" defines detailed technical and organizational requirements for information security systems in financial organizations.

4.2 Comparative analysis of jurisdictions

In its fundamental research, Tursunov BO conducts a detailed comparative analysis of fintech security regulation in different jurisdictions. Particular attention is paid to comparing the approaches in the USA (CCPA), China (PIPL) and Russia (Federal Law on Personal Data) with the regulatory model of Uzbekistan.

Uzbek legislation shows significant similarities with the Russian approach to data localization and national security requirements. At the same time, as noted by MK Abdullaev, the regulatory model of Uzbekistan is more flexible in

relation to cross-border data transfer, which serves to develop international cooperation in the field of fintech.

5. Practical measures of cyber security

5.1 Technical protection measures

According to the requirements of the legislation of Uzbekistan, fintech companies must introduce complex systems of information security. Multi-level data encryption is a mandatory requirement for all financial organizations operating in Uzbekistan. The cryptographic tools used in this should be certified by the competent authorities.

Biometric authentication has achieved special development in the field of Uzbek fintech. The Central Bank of Uzbekistan has developed special requirements for biometric identification systems, taking into account both international experience and national characteristics.

Intrusion detection systems in financial organizations of Uzbekistan must comply with the international standard ISO/IEC 27001:2022, approved by mandatory certification. As Karimov NG noted in his research, the introduction of this requirement significantly increased the security level of the country's banking system .

5.2 Organizational Measures

Shermuhamedov emphasizes the importance of a comprehensive approach to security in IT works. Regular training of employees is becoming a mandatory requirement for financial organizations in Uzbekistan. Central bank regulations require all employees with access to critical systems to undergo information security training on a quarterly basis.

6. The future and challenges of regulation

6.1 Normative development trends

The analysis of current trends in Uzbekistan shows that the development of regulatory legal documents is going in the direction of strengthening the requirements for cloud services. A new law "On Cloud Computing" is being

prepared, which defines special security requirements for the use of cloud technologies in the financial sector.

Regulation of artificial intelligence in fintech is becoming a priority area of legislative development. The Central Bank of Uzbekistan is developing regulations regulating the use of artificial intelligence in financial services, with a special focus on security and protection of consumer rights.

6.2 Adaptation to New Requirements

Uzbekistan's fintech companies actively implement the principle of "Security" by design that meets international standards and national legislative requirements. The development of cyber security culture is supported at the state level through a system of educational programs and professional certification.

7. Summary

The research shows that an effective system has been created in Uzbekistan for the regulation of cyber security in the field of fintech, which successfully combines international standards and national characteristics. The country's experience shows the possibility of creating a balanced regulatory system that ensures both safety and development of innovations.

The main factor of success is the constant improvement of the regulatory framework, taking into account the emergence of new technologies and threats. It is worth noting that the regulatory model of Uzbekistan can be a model for other developing markets seeking to create a modern system of data protection in the financial sector.

REFERENCES

1. Positive Technologies. "Fintech and Security: A Practical Guide", 2023.
2. Central Bank of the Republic of Uzbekistan. "Tizimid Bank Digital Technological and Cybersecurity Situation Report", 2023.
3. Ghulomov SS, Shermuhamedov AT "Digital economy: technological molyavium and cyber security". Tashkent, 2023.
4. Abdullaev MK "The lack of fintech in Uzbekistan: theory and practice"// Economics and innovative technologies, 2023. No. 3.
5. Karimov NG "Tizimid Bank Information Security Issues" // Finance and Bank Ishi Electron magazine, 2023.
6. The Law of the Republic of Uzbekistan "On Personal Data" dated 07.02.2019 No. Zru-547.
7. Tursunov BO "Mechanism of data destruction in fintech companies" // Economy and Education, 2023.
8. Shermuhamedov AT "Information security in the digital economy" // TSEU Bulletin, 2023.
9. ISO/IEC 27001:2022 "Information security management systems - Requirements".
10. Regulation of the Central Bank of the Republic of Uzbekistan "On requirements for ensuring information and cyber security in the implementation of banking operations".
11. World Bank. (2023). Global Fintech Market Report 2023. Washington, DC: World Bank Group.
12. Commentary on the Civil Code of the Republic of Uzbekistan: (second volume. 2013. B. 912, volume 2, edited by HARahmonkulov and O. Akyulov.) Professional reviews. T 2 / Ministry of Justice of the Republic of Uzbekistan. T. Baktriya Press, 2013.
13. Decision PQ-3832 of the President of the Republic of Uzbekistan of July 3, 2018 "On measures to develop the digital economy and the field of crypto-assets circulation in the Republic of Uzbekistan".
14. Abdikhakimov, I. (2023, January). Trademark and copyright infringements in social media. In International Conference on Legal Sciences (Vol. 1, No. 1, pp. 187-200).

15. Abdikhakimov, I. (2023). The Uncertainty Principle: How Quantum Mechanics Is Transforming Jurisprudence. International Journal of Cyber Law, 1(7).
16. Abdikhakimov, I. (2023, June). Unraveling the Copyright Conundrum: Exploring AI-Generated Content and its Implications for Intellectual Property Rights. In International Conference on Legal Sciences (Vol. 1, No. 5, pp. 18-32).