CYBERCRIME AND THE LEGAL PROTECTION OF PERSONAL DATA IN THE DIGITAL SPACE

G‘anijonov Muhammadqodir Sherzodovich
Student at the H.K. Muhitdinova Academic Lyceum under Tashkent State University of Law

Abstract

This article examines the impact of cybercrime on the security of personal data in the digital space and the legal mechanisms for protecting such data. It considers the relevant legislation of the Republic of Uzbekistan on personal data, cybersecurity, and criminal liability, and discusses threats such as unlawful acquisition and disclosure of personal information, phishing, unauthorized account access, and other digital risks. The article also offers proposals for improving legal and organizational safeguards in light of international experience.

Keywords

cybercrime, digital space, personal data, cybersecurity, privacy, phishing, unauthorized access, legal protection, GDPR.

Introduction

The widespread use of the internet and digital technologies means that people leave personal information across electronic services, social networks, mobile applications, and online platforms. Such information can make services more convenient, but if it is unlawfully obtained or disclosed, it may harm a person’s financial interests, reputation, and privacy.

Common forms of cybercrime include obtaining confidential information through phishing messages, unauthorized access to accounts, stealing information with malicious software, and unlawfully acquiring databases. The issue should therefore be considered not only as a technical security challenge, but also in terms of safeguarding individual rights, establishing liability, and creating effective legal remedies. This article aims to analyze the national legal framework for protecting personal data against cybercrime and to develop practical recommendations.

Literature Review

In Uzbekistan, a principal legal source governing the collection, storage, use, and protection of personal data is Law No. O‘RQ-547 of 2 July 2019, “On Personal Data” [1]. The law establishes principles relating to the lawfulness of processing, accuracy, confidentiality, and protection of personal data. It also regulates the circumstances in which data may be disclosed or disseminated, including the need for consent or another lawful basis where applicable.

The Law “On Cybersecurity” establishes legal foundations for protecting information systems and resources from cyber threats [2]. Relevant provisions of the Criminal Code of the Republic of Uzbekistan, including rules addressing offences in the field of information technology and unauthorized access to computer information, are also important for determining criminal liability for certain unlawful acts in the digital environment [3].

At the international level, the European Union’s General Data Protection Regulation (GDPR) provides a systematic framework for lawful processing, data-subject rights, and data security requirements [4]. These sources provide a basis for reviewing national legal mechanisms and comparing them with international approaches.

Research Methodology

The article uses analysis of legal instruments, comparative legal analysis, a systems approach, and synthesis. First, Uzbekistan’s legislation on personal data and cybersecurity, together with relevant provisions of the Criminal Code, was reviewed. Their functions were then compared with the principles of lawful and secure processing reflected in the GDPR. This approach supports practical conclusions on preventing cybercrime and protecting the rights of affected individuals.

Main Analysis

© 2026 International Conference on Artificial Intelligence and Applications . All Rights Reserved.

Cybercrime poses a direct threat to the security of personal data. Criminals may obtain names, telephone numbers, email addresses, bank-card details, passwords, or copies of identity documents and use them to commit fraud, create fake accounts in a victim's name, or attempt to access their accounts. Sometimes information is obtained through a fake website or message that the user believes to be trustworthy. This technique is known as phishing.

The legal protection of personal data requires the lawfulness and purpose of processing to be clear. Law No. O'RQ-547 identifies lawfulness, confidentiality, and protection among the principles governing the processing of personal data [1]. Organizations should therefore collect only necessary information, use it for the stated purpose, and restrict access to authorized persons. Access by an employee or third party without appropriate authorization should prompt a review of security measures.

Legal safeguards are effective when combined with technical measures. Organizations should use strong password policies, multi-factor authentication, encryption during transmission and storage, regular system updates, secure backups, and access controls. When a security incident occurs, it is important to have procedures for recording the incident, assessing its impact, stopping unauthorized access, and contacting the relevant authorities in accordance with applicable law.

Cybersecurity legislation strengthens the organizational and legal framework for protecting information systems and ensuring cybersecurity [2]. The Criminal Code's provisions on offences in the field of information technology address liability for certain unlawful acts [3]. The legal assessment of a particular incident must depend on its facts, the nature of the conduct, and the applicable law. Users can also reduce risk by avoiding suspicious links, never sharing passwords or verification codes, and installing applications only from trusted sources.

The GDPR demonstrates that data protection should not be limited to measures taken after a data breach has occurred [4]. It is important to assess risks before processing data, define the purpose clearly, avoid collecting unnecessary information, and continuously improve security measures. These approaches can also inform national practice through improved internal policies, staff training, and clear privacy notices for users.

Several measures can strengthen legal protection in the digital space. First, digital literacy should be improved, particularly people's ability to recognize phishing and social-engineering techniques. Second, organizations should control access to databases, conduct security audits, and develop incident-response plans. Third, individuals who believe their data have been used unlawfully should have clear, accessible information on how to contact competent authorities or seek judicial remedies. Fourth, cooperation among public authorities, the private sector, and educational institutions can improve prevention and information sharing.

Conclusion

Cybercrime poses a serious threat to the confidentiality, integrity, and security of personal data in the digital space. The unlawful acquisition or disclosure of personal information is not merely a technical problem; it also affects human rights and legitimate interests. In Uzbekistan, the Law "On Personal Data," the Law "On Cybersecurity," and relevant provisions of the Criminal Code form important legal foundations for addressing these issues.

Effective protection requires legal rules to be supported by practical security measures, organizations to monitor their data-processing activities, and citizens to understand digital risks. International principles such as data minimization, prior risk assessment, and protection of data-subject rights can help improve national practice. These steps may strengthen trust in digital services and reduce the risk of unlawful use of personal data.

References

[1] Law of the Republic of Uzbekistan No. O'RQ-547 of 2 July 2019, "On Personal Data." https://lex.uz/docs/-4396419

[2] Law of the Republic of Uzbekistan No. O'RQ-764 of 15 April 2022, "On Cybersecurity." https://lex.uz/uz/acts/-5960604

© 2026 International Conference on Artificial Intelligence and Applications . All Rights Reserved.

[3] Criminal Code of the Republic of Uzbekistan, Chapter XX¹ — Crimes in the Field of Information Technology. https://lex.uz/docs/-111453
[4] Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union, 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj

© 2026 International Conference on Artificial Intelligence and Applications . All Rights Reserved.