

Legal Framework For Personal Data Protection On The Internet

Ismailov Tokhirjon Khushnudbek ugli¹, Karimova Laylo Khushnud kizi²

¹Head of the Chancellery Department at Mamun University

E-mail: ismailovtohir4349@gmail.com

ORCID: 0000-0002-8571-3653

²Karakalpak State University named after Berdakh, Faculty of Law, student in the field of Jurisprudence

Email: I9164665@gmail.com

Abstract: *This article analyzes the legal framework for protecting personal data on the Internet from a scientific and legal perspective. The constitutional and legal foundations of the concept of "personal data," the principles of their processing, the institutional control mechanism, the registry system and the norms of legal responsibility are highlighted. A comparative analysis of the current legislation of the Republic of Uzbekistan in this area, recent amendments, and international experience (GDPR) is scientifically and practically substantiated.*

Keywords: personal data protection, Internet, legal framework, data registry, legal liability, digital security, GDPR, information rights, privacy.

I. Introduction. In the modern digital society, the scope of collection, storage, and dissemination of personal data via the Internet is increasingly expanding, creating serious risks such as interference in citizens' private lives and the illegal dissemination of information [1]. If the vast amount of personal data collected through social networks, electronic services, and various online platforms is not clearly regulated by law, citizens' constitutional rights may be under serious threat.

In recent years, the Republic of Uzbekistan has been implementing consistent legal reforms to regulate this field - the Law "On Personal Data" has been adopted, which has been repeatedly supplemented and amended, including significant changes that further strengthen the protection of personal data [2]. However, the unique, transboundary, and high-speed nature of the Internet requires constant improvement of this legal regulation.

From this perspective, a systematic scientific analysis of the current legal framework for personal data protection on the Internet, its institutional mechanisms, and the legal liability system, as well as the identification of strengths and aspects of existing legislation requiring improvement, determines the relevance of this article [3].

The object of the research is the social and legal relations related to the collection, storage, processing and dissemination of personal data on the Internet. The subject of the study is the legal norms regulating the protection of personal data on the Internet, institutional mechanisms, and the system of legal liability.

II. The level of study of the problem. The international legal framework for personal data protection, including the European Union's GDPR (General Data Protection Regulation), has been extensively covered in the research of foreign lawyers[1], which scientifically substantiates the rights of the data subject and institutions such as the "right to be forgotten." In domestic legal science, the legal nature and fundamental principles of the Law "On Personal Data" are analyzed in the works of legal researchers [2].

Issues of information law and digital security are covered from a general legal perspective in the works of domestic researchers [3], which analyze the negative consequences of personal data disclosure and measures for their prevention. The official materials published by the state body in the field of personal data - the State Personalization Center [4] comment on the main provisions of the current legislation.

Nevertheless, an analysis of the conducted research shows that domestic science still lacks comprehensive scientific and legal research that takes into account the specific characteristics of the Internet (transboundary nature, speed, large number of users) and analyzes all legal mechanisms of local legislation (constitutional, institutional, registry, liability) in a single system [5]. Filling this gap determines the scientific and practical significance of this research.

III. Discussion. When analyzing the legal nature of the concept of "personal data," it is first necessary to refer to its constitutional basis [1]. According to Article 31 of the Constitution of the Republic of Uzbekistan [6], everyone has the right to protection from encroachments on their honor and dignity and interference in their private life. This constitutional norm is developed in detail in the Law "On Personal Data," and according to Article 4 of the Law, personal data is information recorded in electronic form, on paper, or on another material medium that relates to a specific individual or allows for their identification.

The law establishes the fundamental principles of data processing - legality, accuracy and reliability, confidentiality and security, and equality of rights between subjects and operators [2]. It is especially important that, according to Article 15 of the Law, the placement of personal data on the global information network Internet, their disclosure to an indefinite circle of persons is included in the concept of "dissemination" and, as a general rule, can be carried out only with the consent of the subject.

The institutional control mechanism is an important component that ensures the practical functioning of this legislation [3]. The authorized state body in the field of personal data is the State Personalization Center under the Government, which maintains the state register of personal data bases and monitors the activities of owners and operators. Resolution of the Cabinet of Ministers No. 707 dated September 5, 2018, established a procedure for including owners and operators who violate the terms of processing

citizens' personal data on the global information network Internet in a special register and restricting access to their resources—this is carried out in cooperation with the "Uzkomnazorat" State Inspectorate.

The mechanism of legal liability serves as a means of preventive and punitive influence for violations of legal requirements [4]. Article 1412 of the Criminal Code of the Republic of Uzbekistan provides for criminal liability for the illegal disclosure, dissemination, depersonalization of personal data, as well as the failure of the owner and operator to take the necessary legal, organizational and technical measures to protect the data, which is a strict measure introduced in response to the increase in cases of unauthorized use of personal data on the Internet.

Recent amendments to the Law "On Personal Data" have further strengthened this protection system [5] - in particular, it has become mandatory to store biometric, genetic, and telecommunications operator user data within the territory of Uzbekistan. This is an approach partially similar to the principle of limiting cross-border data transfers in the European Union's GDPR regulation, which serves to strengthen national digital sovereignty and the security of citizens' data [1]. At the same time, the implementation of some advanced institutions of the GDPR, such as the "right to be forgotten," in accordance with local legislation can be considered a promising direction.

IV. Results. In the process of analyzing the six main legal mechanisms for the protection of personal data on the Internet, their content, legal basis and practical significance were systematized. The results of the analysis are summarized in the table below:

1-table

Analysis of six main legal mechanisms for protecting personal data on the Internet

№	Legal mechanism	Content	Legal basis	Practical significance
1	Mechanism of constitutional guarantees	Enshrining the right to protection from interference with a person's private life and personal data in a document of the highest legal force	Article 31 of the Constitution of the Republic of Uzbekistan	Creating the highest, immutable legal framework for personal data protection
2	Mechanism for the normative definition of concepts and principles	Defining the concept of "personal data" and the basic principles of its processing at the legislative level	Article 4 of the Law "On Personal Data" and other relevant articles	Creation of a system of clear, uniformly understood legal concepts for subjects of law
3	Institutional control mechanism Institutional control mechanism	Determination of the authorized state body in the field of personal data and its supervisory powers	Norms regulating the activities of the authorized state body (State Personalization Center) and the "Uzkomnazorat" inspection	The existence of an institutional mechanism for identifying and eliminating violations of the law
4	Registry and registration mechanism	Registration of personal databases in the state register, inclusion of offenders in the special register	Resolution of the Cabinet of Ministers No. 707 dated September 5, 2018, and the relevant registry procedures	Bringing the activities of owners and operators into a transparent and controlled state
5	Restriction and blocking mechanism	Restriction or suspension of access to Internet resources that violate legal requirements	Access restriction procedures provided for by Cabinet of Ministers Resolution No. 707	The ability to promptly take action against resources that disseminate information in violation of the law
6	Legal liability mechanism	Establishing criminal and administrative liability for the illegal disclosure, dissemination, or failure to take measures to protect personal data	Article 1412 of the Criminal Code of the Republic of Uzbekistan, relevant norms of administrative liability	Presence of a preventive and punitive legal remedy for an offense

As seen from the analysis presented in Table 1, an integrated system of legal mechanisms for personal data protection has been formed in the Republic of Uzbekistan, ranging from the constitutional basis to institutional control and legal liability. These mechanisms are inextricably linked, with each performing its own specific functional function.

The results of the analysis also showed that the legislation has been consistently improved in recent years, particularly through amendments in 2021 and 2026, which indicates the state's desire to respond quickly to new challenges in the digital space (biometric data security, cross-border transmission issues). Overall, the analysis confirmed that the core elements of the existing legal system are fully formed, but further enrichment with international best practices (GDPR) is a promising direction.

V. Results and statistical analysis.

The research results demonstrated that the issue of personal data protection on the internet is relevant not only theoretically and legally but also practically. In the Republic of Uzbekistan, alongside the expansion of digital services and internet access, a sharp increase in the number of offenses committed using information technologies is being observed. Based on a comparative analysis of official open data, the following results were formed.

2-table

Some statistical indicators of risks associated with the Internet and information technology in Uzbekistan

№	Statistical indicator	Result	Analytical significance
1	Number of Internet users in Uzbekistan	More than 31 mill.	This indicates that the scope of personal data processing in the digital environment has expanded.
2	Crimes committed using IT in 2019	863	Comparative baseline indicator of cybercrime
3	Crimes committed using IT in 2024	58 800	This indicates a sharp increase compared to 2019.
4	Share of cybercrimes in the total number of crimes in 2023	6,2 %	Represents the role of cybercrime in the overall structure of crime
5	Share of cybercrimes in the total number of crimes in 2024	44,4 %	The share of cybercrimes has increased significantly over the year.
6	The share of bank card fraud and cyber theft in cybercrime	98 %	Indicates that financial and identity information is at high risk
7	Mobile device users who are exposed to influence aimed at gaining personal information through fake calls	about 95%	This indicates the widespread use of social engineering methods.
8	Funds embezzled from citizens as a result of cybercrimes	Over 1.909 trillion soums	Indicates the high economic consequences of cyber threats
9	According to the analysis, the circumstances that created the conditions for the commission of the crime without the victim's knowledge	95 %	Indicates the need to increase legal and cybersecurity literacy

Analysis of the data in Table 2 shows that with the acceleration of the digitalization process in Uzbekistan, the illegal acquisition of personal data, its use for fraudulent purposes, and factors threatening the digital identification of citizens are also increasing. Specifically, while the number of crimes committed using information technology was 863 in 2019, this figure reached 58,800 in 2024. According to estimates, the number of such crimes has increased nearly 68.1 times over five years [7].

In particular, the share of cybercrime in the structure of total crime is an important indicator. While this figure stood at 6.2% in 2023, it reached 44.4% in 2024. Thus, over the year, the share of cybercrimes in the total number of crimes increased by 38.2 percentage points, that is, in terms of share, it increased almost 7.2 times. This situation indicates that crime is rapidly moving from traditional forms to the digital environment.

Another aspect that should be considered in the analysis is that 98 percent of cybercrimes are fraud or cybertheft related to bank cards. The illegal acquisition of phone numbers, bank card details, verification codes, and other identification data remains one of the important risk factors in committing this type of crime. Therefore, it is not enough to limit the protection of personal data only to the technical security of databases. Interconnected legal regulation is required regarding the provision of data by citizens to third parties, the storage and processing of data by operators, and liability in the event of data breaches.

Statistics indicate that in 95% of cybercrimes, citizens provide personal data to fraudsters or install malicious software due to insufficient cybersecurity knowledge, which creates conditions for the commission of crimes. This indicates that improving legal protection mechanisms for personal data, as well as increasing digital and legal literacy, is an important area of prevention.

The results obtained show that although the basic legal framework for the protection of personal data has been formed in Uzbekistan, the rapid change of risks in the digital environment requires constant improvement of legislation and its enforcement mechanisms. In this regard, it is advisable to strengthen the responsibility of data operators, apply effective legal measures against

cases of illegal processing and dissemination, strengthen identification and authentication requirements in information systems, and expand the capabilities of citizens to control personal data. Statistical analysis has shown that the issue of protecting personal data on the Internet is a complex legal problem directly related to cybersecurity, ensuring the inviolability of private life and property interests of citizens. The sharp increase in the number of cybercrimes necessitates adapting existing legal mechanisms to modern digital threats, strengthening preventive measures, and increasing the legal responsibility of entities handling personal data.

VI. Conclusion. The legal framework for the protection of personal data on the Internet has been formed in the Republic of Uzbekistan as an integrated system consisting of constitutional guarantees, legal regulation, institutional control, a registry system, a restriction mechanism, and legal liability. Research results have shown that this system has been consistently improved in recent years, but the rapid development of digital technologies requires its constant updating.

Studying and implementing international best practices, specifically adapting certain institutions in the European Union's GDPR regulation to local conditions, is a promising direction for further improving legislation. In future research, it is advisable to study the legal aspects of personal data protection in the context of new technologies on the Internet (artificial intelligence, big data).

VII. References:

1. European Union. Regulation (EU) 2016/679 (General Data Protection Regulation). – Brussels: Official Journal of the European Union, 2016. <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
2. Law of the Republic of Uzbekistan "On Personal Data," dated 02.07.2019 No. ZRU-547. <https://lex.uz/docs/-4396419>
3. Ministry of Internal Affairs of the Republic of Uzbekistan. Negative aspects of personal data disclosure and measures to prevent them. - Tashkent, 2023. <https://pd.gov.uz/posts/view?id=13>
4. State Personalization Center under the Republic of Uzbekistan. State Register of Personal Databases. – pd.gov.uz, 2024. <https://pd.gov.uz/>
5. Resolution of the Cabinet of Ministers of the Republic of Uzbekistan No. 707 dated September 5, 2018, "On measures to further improve information security on the World Wide Web." <https://lex.uz/uz/docs/-3893085>
6. Constitution of the Republic of Uzbekistan. 01.05.2023. <https://lex.uz/docs/-6445145>
7. Creating a Safe Cyberspace by Combating Cybercrime. Uzbekistan's experience in the early prevention of cybercrime in the context of digital transformation. Uzbekistan's Experience in Preventing Cybercrime and Ensuring a Safe Cyberspace. <https://gov.uz/en/iiv/news/view/52319>