E-ISSN: 2997-9382

SemantJournals

American Journal of Technology Advancement

https://semantjournals.org/index.php/AJTA

| Research Article

Check for updates

Protection of Personal Data in Civil Law: the Concept of Digital Identity

Javokhir Eshonkulov

Tashkent State University of Law, Lecturer at the Department of Cyber Law, Uzbekistan

javohireshonqulov0724@gmail.com

Farmonov Sunnatillo Utkir O‘g‘li

Tashkent State University of Law, 2nd-year student of the International Law and Comparative Legislation

sunnatillofarmonov606@gmail.com

Annotation

This article analyzes the civil law issues and shortcomings related to the protection of personal data, the efforts undertaken by Uzbekistan in this field, international experiences, and the concept of digital identity.

Keywords: personal data, personal data protection, personal rights, data security, digital identity.

Introduction

In the digital era, the protection of personal data has become a pressing issue. The collection, processing, and storage of personal data by various organizations sometimes lead to breaches of confidentiality and security. It is no longer surprising that platforms using such data experience malfunctions or cyberattacks. Therefore, in today’s information-driven world, the value of personal data continues to increase. In Uzbekistan, mechanisms for protecting such data through national legislation, learning from international experience, and preparing technical safeguards against cyber threats are being developed step by step.

Now, let us focus on the core of our topic—personal data. What is personal data? What information falls under this category?

Personal data refers to all information that enables the identification of an individual, including name, surname, passport details, phone number, email address, biometric data, medical records, and more. The primary objective of personal data protection in civil law is to ensure the inviolability of personal life and to prevent and safeguard against violations of individual rights.

From a legal perspective, the definition of personal data can be found in Article 4 of the Law of Uzbekistan "On Personal Data." According to this law, personal data refers to information recorded in electronic, paper, or other material forms that relate to a specific individual or allow

for their identification. Such data can be found in identity documents (passport, ID), electronic government platforms (e.g., my.gov), or employee databases within organizations.

Both government and private entities process personal data under specific conditions. The government uses such data for interactive services, labor relations, and security matters, while private organizations may use them for various purposes, subject to authorization.

Several key conditions must be met in this process. First, the collection and processing of personal data require the individual's consent. Second, the use of collected data must be lawful and purpose-driven. Unauthorized use of data can lead to legal consequences. Additionally, appropriate security measures must be taken to ensure data confidentiality and protection.

Individuals have the right to access, modify, delete, and restrict the processing of their data at their discretion.

Methods: Legal Framework for Personal Data Protection in Uzbekistan.

Uzbekistan has established several legal foundations for personal data protection, including:

- The Law "On Personal Data"
- Article 31 of the Constitution of Uzbekistan
- Articles 99 and 1179 of the Civil Code of Uzbekistan

According to the above regulations, every person has the right to personal and family privacy, the confidentiality of electronic and other correspondence and messages, and, in general, the security of personal data is guaranteed by law. Nevertheless, there are several issues in protecting personal data. Let’s examine them one by one:

The first issue is the complexity of legal documents. Due to the highly complex and incomprehensible nature of laws, ordinary citizens may not fully understand their rights. Where laws exist, they are often complicated and difficult for ordinary people to grasp. This complexity prevents individuals from fully exercising their rights and reduces the effectiveness of the legal protection measures available to them. Therefore, raising public legal awareness and legal culture should be carried out at the initiative of legal professionals.

The next issue is the violation of citizens’ personal rights, such as the unauthorized use of personal data. Collecting, storing, and processing personal data without the owner's consent is a common problem. In such cases, unauthorized use can lead to privacy violations and the misuse of personal information. Unfortunately, another frequent issue in our society is the spread of false information. The dissemination of false or misleading information can significantly harm a person’s reputation and lead to various personal and professional consequences. However, such actions are protected against at the constitutional level, with corresponding administrative and criminal liabilities established.

Data security has become a pressing global issue. Cyberattacks, data breaches, and other security threats in the digital space remain insufficiently addressed. Personal data is frequently targeted by cyberattacks, leading to breaches of confidential information. Many organizations lack robust security measures to protect against such threats, making personal data vulnerable to exposure and misuse.

Professor A. Niyozov emphasizes that when rights related to a person’s name, personal inviolability, home privacy, appearance and image, medical confidentiality, attorney-client privilege, adoption secrecy, correspondence, and telephone conversations are violated, lawmakers declare legal protection. However, they often fail to establish concrete liability measures. As a result, perpetrators do not face additional personal or financial obligations or inconveniences.

One of the most widespread fraud types today is remote scams, where criminals use phone calls to commit various fraudulent activities, clone personal data, steal money from bank accounts, or take online loans using stolen personal information. Catching offenders is also challenging, as they often avoid using phone numbers, IP addresses, or accounts registered under their names. The negligence of citizens also contributes to the increasing prevalence of such crimes.

As time progresses, personal data is increasingly being compromised through new technological tools. This sometimes leads to a shortage of technological resources needed to ensure data security. The lack of necessary technological tools or the obsolescence of existing ones makes the problem even more challenging. The rapid pace of technological advancement can render current data protection measures outdated. Constant updates to these measures require financial investment.

Regarding accountability, there are concerns about the adequacy of measures taken in response to violations. Punishments may not always be severe enough, and even when violations are detected, the penalties imposed may not be sufficient to deter future offenses. Additionally, as mentioned earlier, there are challenges in apprehending those who commit such violations.

Managing personal data, obtaining consent, and ensuring transparency are crucial issues. Citizens must be aware of how their data is being used and should have a clear and transparent process for providing consent. However, consent procedures are often vague, and people may not fully understand what they are agreeing to. A simple example is when we accept the terms and conditions of a website without reading them carefully, thereby unknowingly sharing our data.

Furthermore, individuals should have the right to update or delete their personal data. However, exercising these rights can be difficult. Organizations may continue to circulate outdated or incorrect data. The right to one's name is one of the most fundamental non-property rights that ensures individual identity.

Results: To address these challenges effectively, we can examine successful international approaches. Strengthening our legal framework by adapting foreign data protection laws and systems to our national context can be beneficial. Several successful regulations and legal frameworks exist worldwide for protecting personal data.

For example, in 2018, the European Union (EU) introduced the General Data Protection Regulation (GDPR). GDPR establishes clear rules for collecting, storing, using, and sharing personal data. Its primary goal is to ensure transparency in data usage and protect users from harmful or illegal data practices. GDPR also imposes strict obligations on companies, including obtaining users' consent before collecting data, ensuring data security, and protecting the rights of individuals affected by data breaches. Additionally, violations of GDPR result in significant penalties and financial fines.

In the United States, there are also several laws dedicated to personal data protection. For instance, the California Consumer Privacy Act (CCPA) introduces a new approach to safeguarding personal data. This law aims to provide users with full control over their data and requires companies to maintain transparency in handling personal information. Since this regulation is part of California's legal framework, other states have adopted similar approaches to personal data protection.

Protection of Personal Data in the Republic of Uzbekistan

The Republic of Uzbekistan is paying great attention to the protection of personal data. In 2021, the country adopted the Law "On Personal Data," which establishes clear rules for the collection, use, storage, and protection of personal data. This law provides a broad perspective on the necessity of obtaining consent for data dissemination, the rights of data subjects, and the role of state regulatory bodies overseeing data protection.

Discussion: Uzbekistan is actively implementing new technologies to enhance personal data protection. For instance, state institutions are introducing digital identification systems and developing electronic government services, which ensure data security while facilitating citizens' access to various services. Additionally, the Ministry for the Development of Information Technologies and Communications of Uzbekistan is continuously making changes and updates to ensure data security. These initiatives aim to protect users' personal information and guarantee its safety.

Globally, personal data is protected through various laws and technologies. International practices, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), set high standards for data protection. Uzbekistan is also taking significant steps in this area by implementing legal and technological advancements. Personal data protection is crucial in modern society, as it not only safeguards citizens' rights but also fosters trust in both the public and private sectors.

Today, the concept of **"Digital Identity"** plays an essential role in personal data protection. A digital identity represents an individual's virtual presence in the digital world, formed through social networks, electronic services, mobile applications, and other digital platforms.

Digital footprints refer to all user activities on the internet, including social media engagement, online purchases, and search queries. These footprints contribute to the formation of an individual’s digital identity. For example, when a person shares aspects of their daily life on social media, enters their name, surname, and address during online purchases, or interacts with personal data-related offers on websites, they leave digital traces.

Identification and authentication are key to verifying digital identities. Technologies such as logins, passwords, and biometric data are used for this purpose, as they enable individuals to navigate the digital world securely.

Digital reputation is shaped by a person’s online activities and interactions. However, challenges exist in protecting digital identities:

1. Digital identity theft (e.g., phishing attacks): One of the most common types is email phishing, where fraudsters send fake emails and direct users to counterfeit websites to steal personal data.

Another type is vishing, where scammers attempt to obtain personal information through phone calls.

2. Illegal distribution or misuse of personal data: Personal data is often shared without consent through digital footprints, potentially harming an individual's digital reputation. This issue is particularly prevalent on social media platforms like Instagram and Telegram.

Conclusion:

In civil law, the protection of personal data and the concept of digital identity are crucial for safeguarding human rights, ensuring personal privacy, and enhancing digital security. Therefore, both state institutions and the private sector must comply with legal requirements and international standards when handling personal data.

References:

1. Eshonkulov, J. (2025). The Role of Smart Contracts in Civil Law and Issues of Legal Regulation. Uzbek Journal of Law and Digital Policy, 3(1), 104–111. https://doi.org/10.59022/ujldp.294
2. Eshonkulov, J. (2024). Legal Foundations for the Application of Artificial Intelligence Technologies in the Sports Industry. American Journal of Education and Evaluation Studies, 1(7), 240-247. https://semantjournals.org/index.php/AJEES/article/view/320/287

3. Law of the Republic of Uzbekistan "On Personal Data"
4. Tog‘aymurodova, B. Ch. (2024). Civil Law Issues in Personal Data Protection. Modern World Social Sciences: Theoretical and Practical Research, Online Conference, pp. 10-13.
5. Nasriyev, I. (2006). Issues of Exercising and Protecting Personal Non-Property Rights in Civil Law. Dissertation, Tashkent, p. 88.
6. GDPR Summary (gdprsummary.com)
7. State of California - Department of Justice, updated on March 13, 2024
8. Ismatov, O. Sh. (2024). Personal Data: Foreign and Local Experience. Senior Specialist, Department of International Cooperation, Center for Legal Training, Ministry of Justice of Uzbekistan.