SCIENCEZONE | ONLINE SCIENTIFIC CONFERENCES

CRIMINAL LAW AND CRIMINOLOGICAL ASPECTS OF THE UNLAWFUL USE OF PERSONAL DATA DATABASES

Avazbek Sayfiddinov
Junior Researcher, Research Center, Faculty of Criminal Justice, Tashkent State University of Law
avazbeksayfiddinov23@gmail.com

Abstract. This article analyzes the criminal law and criminological aspects of the unlawful use of personal data databases in the context of digitalization. It examines the social danger of such acts, their criminal law characteristics, and criminological features under the legislation of the Republic of Uzbekistan. Attention is paid to Article 141² of the Criminal Code of the Republic of Uzbekistan, as well as the relevant provisions of the Law "On Personal Data" and administrative liability legislation. The article also provides a comparative analysis of the Uzbek legal framework with the requirements of the European Union's General Data Protection Regulation (GDPR) and Convention 108 of the Council of Europe. Based on the comparative analysis, proposals are developed to strengthen preventive, organizational, and legal mechanisms for protecting personal data in Uzbekistan.

Keywords: personal data, database, unlawful use, cybercrime, criminal liability, criminology, GDPR, data security.

Introduction

The expansion of digital government, banking, e-commerce, and online services has turned personal data into a digital resource of significant economic value. Because full names, passport details, telephone numbers, and biometric and genetic data are now consolidated within unified databases, their unlawful use can simultaneously infringe upon the rights of a large number of individuals. Under Uzbek legislation, personal data is defined as information relating to a specific natural person or information that makes it possible to identify that person (Law of the Republic of Uzbekistan No. O'RQ-547, 2019, Art. 4). The core problem is that unlawful access to a database is rarely an end in itself: stolen data is typically reused for fraud, fraudulent loan applications, account takeover, extortion, or invasion of privacy. Consequently, this offense is not merely an information-security concern but a criminal law phenomenon that infringes upon an individual's rights and freedoms.

Article 141² of the Criminal Code of the Republic of Uzbekistan establishes criminal liability for the unlawful collection, systematization, storage, alteration, supplementation, use, disclosure, distribution, transfer, alienation, and destruction of personal data (Criminal Code of the Republic of Uzbekistan, Art. 141²). This provision is of a blanket (reference) nature, meaning that the Law "On Personal Data" and its subordinate norms are decisive in establishing the unlawfulness of the act. Uzbekistan's model is based on a coherent system of administrative and criminal liability: Article 46² of the Code of Administrative Liability establishes administrative liability for the relevant offenses, while Article 141² of the Criminal Code provides for criminal liability in certain cases following the prior imposition of an administrative penalty (Code of Administrative Liability of the Republic of Uzbekistan, Art. 46²; Criminal Code of the Republic of Uzbekistan, Art. 141²). Liability is aggravated by commission in a group, repetition, mercenary motive, abuse of an official position, and the occurrence of grave consequences.

However, the principal weakness of this criminal law protection is that the harm caused rarely ends with the theft of the data itself. This is particularly true of biometric data: unlike an ordinary password, it cannot readily be replaced once compromised. The concept of harm should therefore

not be limited to material loss but should also encompass threats to identity security, privacy, and future legal interests. From a criminological standpoint, these offenses are characterized by concealment, the use of intermediaries, and multi-stage execution. An offender may obtain data through an insider within an organization, a contractor, a vulnerability in an information system, or phishing. The simplistic notion of "the offender as a technical specialist" is therefore insufficient: the person who obtains the data, the person who sells it, and the person who subsequently uses it in the commission of another offense may all be different individuals. Nor is the victim necessarily limited to persons with low digital literacy — a single database breach can give rise to mass victimization.

The European Union's GDPR model provides an important comparative benchmark for Uzbekistan. The GDPR establishes the principles of lawfulness, transparency, purpose limitation, data minimization, storage limitation, integrity, and confidentiality (General Data Protection Regulation, 2016, Art. 5). It further requires technical and organizational measures proportionate to risk, including encryption, pseudonymization, ensuring the ongoing confidentiality and integrity of systems, and regular testing of security measures (General Data Protection Regulation, 2016, Art. 32).

The Council of Europe's Convention No. 108 likewise requires that data be obtained lawfully, stored for a specified purpose, not be excessive, and be subject to appropriate security measures (Council of Europe, 1981, Arts. 5 –7). A distinguishing feature of the international approach, compared with the Uzbek model, is that alongside liability it places "privacy by design," prior risk assessment, and technical-organizational protection at the center of the framework.

In Uzbekistan, Law No. O'RQ-1125 of 26 March 2026 introduced additional requirements for storing biometric and genetic data, as well as user data held by telecommunications operators, within the territory of Uzbekistan (Law of the Republic of Uzbekistan No. O'RQ-1125, 2026). This is a positive step from the standpoint of data sovereignty; however, the domestic storage of data does not, by itself, automatically prevent its unlawful use.

CONCLUSION

The unlawful use of personal data databases represents an infrastructural form of digital crime. Although Article 141² of the Criminal Code creates the

necessary criminal law foundation, a model relying on punishment alone is not sufficient. For Uzbekistan, it would be appropriate to strengthen role-based access control within databases, multi-factor authentication, audit logging, insider-risk assessment, and mechanisms for the prompt notification of data breaches. International experience shows that the actual level of protection depends less on where data is stored than on the ability to control who accessed it, when, and why, and how quickly unlawful use can be detected.

REFERENCES

1. Code of Administrative Liability of the Republic of Uzbekistan, Art. 46².

2. Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

3. Criminal Code of the Republic of Uzbekistan, Art. 141².

4. General Data Protection Regulation, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, Arts. 5, 25, 32.

5. Law of the Republic of Uzbekistan No. O'RQ-547. (2019, July 2). On Personal Data.

6. Law of the Republic of Uzbekistan No. O'RQ-1125. (2026, March 26). On Amendments and Addenda to the Law "On Personal Data."