International Journal of Scientific Trends- (IJST)
ISSN: 2980-4299
Volume 5, Issue 1, January - 2026
Website: https://scientifictrends.org/index.php/ijst
Open Access, Peer Reviewed, Scientific Journal

Theoretical And Practical Aspects of Crime Prevention in the Field of Personal Data

Choriev Anvar Kuzievich,
Independent Researcher of Tashkent State University of Law
E-mail: anvarkuzievich@gmail.com

Abstract

The article examines the theoretical and methodological foundations of crime prevention and reveals its significance in the life of society. The role of studies on the causes of crime, conditions facilitating its commission, the mechanism of individual criminal behavior, and criminological forecasting within the system of crime prevention is analyzed. The author refers to the scientific and philosophical origins of the idea of crime prevention, highlighting the views of foreign thinkers who assigned priority importance to preventive activities.

Furthermore, the article clarifies the correlation and distinction between the concept of crime prevention and general and special prevention, and characterizes social, criminological, and individual types of preventive measures. Particular attention is paid to substantiating that an increase in the level of legal awareness and legal culture constitutes a key factor in preventing crimes related to violations of personal data legislation. It is emphasized that the level of crime is directly dependent on the state of legal culture in society. Based on an analysis of the content of the Decree of the President of the Republic of Uzbekistan aimed at enhancing legal awareness and legal culture, the article substantiates the necessity of ensuring systemic consistency and continuity in the education system, as well as forming legal immunity among young people.

Keywords: Crime, crime prevention, prevention, individual prevention, legal awareness, legal culture, personal data, rule of law, legal education of youth.

Introduction

The study of the causes of crime and the conditions facilitating it, the mechanisms of individual criminal behavior, and criminological research aimed at forecasting crime are all essential prerequisites for the effective prevention of criminality.

The idea that crime prevention should prevail over the state's punitive policy was first articulated by Plato, who maintained that society should operate under a well-designed legal system capable

of deterring individuals from committing crimes. In the eighteenth century, prominent Enlightenment thinkers such as Charles de Montesquieu and Cesare Beccaria formulated the principle that a wise legislator should focus not on punishing crimes, but on preventing them, primarily through the moral improvement of society. Voltaire further advanced the fundamentally important idea that the prevention of crime constitutes true jurisprudence in a civilized society. The validity of these principles has been confirmed by subsequent generations of theorists and practitioners engaged in combating crime.

The concept of crime prevention is broader than the notions of general and special prevention traditionally associated with punishment in criminal law. Crime prevention is understood as a set of diverse and interrelated measures adopted by both state authorities and public organizations. These measures are aimed at directly or indirectly eliminating the causes of crime, the conditions conducive to its commission, as well as other manifestations of social pathology.

Achieving these objectives presupposes the resolution of a system of hierarchically interconnected tasks. The first task involves preventive influence on the overall structure, dynamics, and causes of crime (social prevention). The second task concerns the prevention of specific types and forms of criminal behavior, crimes committed in particular spheres of social life, as well as offenses perpetrated by certain social groups (criminological prevention). The third task consists in preventing crimes committed by specific individuals (individual criminological prevention). The resolution of the first task extends beyond the scope of criminology and constitutes an integral part of social life as a whole, as well as the subject matter of all disciplines concerned with crime control. Criminology, in turn, focuses directly on that segment of social practice which involves conduct prohibited by criminal law.

Crime prevention is carried out through various forms of preventive activity, among which prophylaxis occupies a leading position[1]. In order to achieve effective results in crime prevention, reduce the number of crimes, and eliminate negative consequences, it is first necessary to study the phenomena, events, and processes that necessitate the existence and development of crime in society and influence it, acting as its causes, as well as the causal relationships between them.[2] Prophylaxis is aimed at preventing specific crimes and restraining individual members of society from engaging in unlawful behavior. The distinctive features of preventive measures implemented within this framework are as follows: first, they are closely linked to specific causes and conditions; second, they are designed precisely to eliminate or neutralize those causes and conditions; third, the prevention of crime constitutes their primary, and in some cases their sole, substantive content.

The prevention of crimes related to violations of legislation on personal data primarily depends on enhancing the level of legal awareness and legal culture. The continuous development of legal awareness and legal culture in society is one of the most important prerequisites for ensuring the supremacy of law and strengthening legality.

In the absence of legal immunity to factors negatively affecting legal education—particularly among young people—criminal behavior becomes entrenched in society to the extent that it is perceived as part of everyday social relations.

Legal awareness represents a form of an individual's conscious attitude toward law, expressed in respect for legislation, understanding of legal requirements, and the ability to comply with them.

Legal culture, in turn, constitutes the practical manifestation of legal knowledge and a responsible attitude toward the law.

The higher the level of legal culture in society, the lower the rate of crime. Legal culture is not merely a form of individual legal knowledge, but rather an indicator of the overall legal environment of society.

In the Decree of the President of the Republic of Uzbekistan devoted to enhancing legal awareness and legal culture in society, it was emphasized that particular attention should be paid to the systematic and continuous implementation of education and upbringing. This process should begin from the preschool education system and aim to deeply instill legal awareness and legal culture among all segments of the population, while broadly promoting the idea of maintaining a balance between individual and public interests [3].

The Concept for Enhancing Legal Culture in Society, approved by the said Decree, notes that a number of problems and shortcomings continue to hinder the formation of respect for human rights and freedoms, the development of legal awareness and legal culture, and the improvement of citizens' legal literacy. In particular, it highlights that efforts to enhance legal awareness and legal culture are not organized in a systematic and integrated manner; legal education is not harmonized with the continuous education system; effective cooperation mechanisms with non-governmental non-profit organizations and other civil society institutions have not been established; targeted measures to develop legal immunity among youth against factors negatively affecting their legal education have not been defined; the active participation of state bodies and sectoral services in organizing and implementing targeted legal outreach activities is not sufficiently ensured; innovative methods of legal advocacy, including web technologies, are not adequately utilized; and legal mechanisms for encouraging projects aimed at increasing legal literacy are lacking.

Unfortunately, crime statistics in Uzbekistan continue to indicate the existence of a number of systemic problems in combating crime. According to data from the Senate of the Oliy Majlis of the Republic of Uzbekistan, in 2024 a total of 132,298 crimes were committed nationwide, with approximately 200 crimes per 100,000 population. Crimes that could have been prevented still constitute a significant proportion of total crime. The largest share of preventable crimes consists of theft and fraud, with 59.4 percent committed by young people and 36.1 percent by previously convicted individuals.

In addition, it was noted that more than 7,000 crimes were committed by unemployed persons, indicating that issues related to employment at the local level are not being addressed effectively. In the field of cybersecurity, 58,800 crimes were recorded, 97.7 percent of which were associated with the unlawful acquisition of funds from citizens' bank payment cards, which has been subject to serious criticism[4].

An analysis of the above data demonstrates that cybercrime accounts for 44.5 percent of all recorded crimes, and this figure is increasing annually. The study further reveals that offenses involving violations of legislation on the processing of personal data are predominantly committed in cyberspace, which necessitates a particularly responsible and targeted approach to the prevention of such crimes.

In many cases, the term crime prevention is used interchangeably with prophylaxis. According to Q. Abdursalova, numerous views have been expressed in specialized literature regarding the concept of crime prevention or crime prophylaxis. However, the most widely accepted definition

characterizes it as “measures or a system of measures undertaken by state and public authorities and organizations aimed at eliminating or neutralizing the causes and conditions of crime.” In the author’s view, it is impossible to deny the close interrelationship between the concepts of “crime prevention” and “crime prophylaxis.” While “crime prevention” represents a relatively general concept, “crime prophylaxis” emphasizes the role of specific measures aimed at preventing criminal behavior[5].

We also concur with this viewpoint and emphasize that prophylaxis represents the implementation of specific and targeted measures. This position is justified by the existence of the Law of the Republic of Uzbekistan “On the Prevention of Offenses,” which identifies general, special, individual, and victimological types of offense prevention.

Pursuant to Article 23 of the said Law, general prevention of offenses is carried out through the development and implementation of state and other programs related to offense prevention; the dissemination of legal awareness among the population; the identification and elimination of the causes of offenses and the conditions facilitating their commission; and the submission of official recommendations aimed at eliminating such causes and conditions.

Based on this legal framework, a number of measures have been implemented to prevent crimes involving violations of legislation on the processing of personal data (LPDP) as part of general preventive activities. In particular, the Laws of the Republic of Uzbekistan “On Personal Data,” “On Cybersecurity,” and “On Informatization” have been adopted, along with the Presidential Decree approving the “Digital Uzbekistan–2030” Strategy and measures for its effective implementation. In addition, several presidential resolutions have been enacted, including those on the introduction of a system for training professional personnel to combat crimes committed using digital technologies; on the organization of scientific research in the field of digital forensics; and on strengthening the protection of the rights of consumers of digital products (services) and combating offenses committed through digital technologies. Relevant research activities are also being conducted.

Nevertheless, despite the measures taken, the number of cybercrimes, including crimes related to personal data, continues to increase.

Improving the Legal Framework for the Prevention of Crimes Involving Personal Data.

At present, notwithstanding the existence of an extensive regulatory and legal framework, crimes against personal data are characterized by rapid and unpredictable development. Technological progress is advancing at an exceptionally fast pace, resulting in the emergence of new concepts, systems, and mechanisms. While modern society quickly assimilates these innovations, legislation often fails to keep pace in terms of timely regulation and legal clarification.

In particular, offenses in the field of information technologies are evolving rapidly. Despite a broad legal framework, statistics on offenses committed in the virtual environment remain high and demonstrate a steady upward trend.

In recent years, within the framework of ongoing reforms, special attention has been paid to the digitalization of all sectors and the establishment of a genuine information society in Uzbekistan. Specifically, through the unified portal my.gov.uz, more than 8 million citizens and entrepreneurs currently utilize over 570 types of online public services.

The Unified Identification System of e-Government (id.egov.uz) has been introduced, enabling citizens to access more than 245 information resources of state bodies. At the same time, extensive digital transformation is being carried out in the banking and financial services sectors.

The "Uzbekistan–2030" Strategy sets ambitious objectives, including increasing the share of public services provided in electronic form to 100 percent, raising the proportion of services delivered exclusively through the Unified Interactive Public Services Portal to 50 percent, and expanding the number of public services provided in a composite and proactive manner to at least 40.

Analytical data indicate that as digitalization and the information technology sector continue to develop, the relevance of ensuring cybersecurity—including the protection of personal data—is increasing accordingly. According to the Cybersecurity Center, more than 12 million attempted cyberattacks were recorded in Uzbekistan in 2024.

Furthermore, it has been established that cybercrimes and crimes related to personal data are primarily committed using the following methods:

• obtaining bank card confidential codes through fraudulent links sent under the guise of financial assistance, online loans, or lottery winnings (34 percent);

• acquiring victims' funds by securing advance payments without returning the money or fulfilling contractual obligations (22 percent);

• impersonating employees of payment companies (such as Click and others) or bank security services during phone calls in order to obtain card numbers and confidential codes (17 percent);

• disclosure of card numbers and codes through online trading platforms (14 percent);

• commission of crimes through fake online financial exchanges (9 percent).

Analysis of National Legislation Aimed at Ensuring the Security of Personal Data.

An analysis of national legislation aimed at ensuring the security of personal data has revealed the following ambiguities and shortcomings:

1. The procedure for real-time information exchange among state authorities, banks, and telecommunications operators regarding incidents of personal data theft, unlawful acquisition, and cybersecurity breaches has not been clearly established.

2. Measures to protect citizens from crimes committed through the use of information and communication technologies have not been defined at the legislative level.

A study of the experience of foreign countries (including Russia, Kazakhstan, Ukraine, and European states) demonstrates that a number of measures to combat offenses against personal data committed through information and communication technologies are regulated at the legislative level. In particular:

•In the Russian Federation, a unified state information system has been established to combat cybercrime [6];

• In Ukraine and the United States, the sending of mass communications without user consent is prohibited [7];

• In the Russian Federation and Ireland, a "trusted representative" mechanism is applied in the execution of online banking transactions [8].

Based on the above, it is proposed to:

• expand real-time data exchange capabilities among state authorities, banks, and telecommunications operators;

• provide citizens with the opportunity to appoint a trusted representative to authorize electronic (online) money transfers, whereby funds cannot be transferred from an account without the consent of such a representative;

• impose an obligation on telecommunications operators to connect to anti-fraud systems in the course of service provision and establish administrative liability for failure to comply with these requirements;

• regulate mass calls and bulk communications.

Organizational and Technical Aspects of Preventing Crimes Related to Personal Data.

Organizational measures.

It is necessary to strengthen the activities of a specially authorized state body responsible for data protection. Its functions should include:

• monitoring information security;

• reporting violations of a criminal nature to law enforcement agencies and the прокурaтор's office;

• conducting inspections and compliance audits;

• providing organizational and methodological assistance to personal data subjects.

At the same time, all public and private organizations should appoint a responsible officer for personal data protection (Data Protection Officer – DPO). This practice, inspired by the standards of the European Union's General Data Protection Regulation (GDPR), enhances personal accountability in the handling of personal data.

There is a shortage of qualified specialists in the fields of information security, cybercrime prevention, and personal data protection. Therefore, it is necessary to introduce specialized educational courses at higher education institutions and implement retraining programs for current employees.

Public awareness efforts regarding the importance of personal data protection, associated risks, and criminal consequences should be conducted on a systematic basis. In this process, the involvement of mass media, social networks, local councils, and community representatives would be particularly effective.

Technical measures.

The following technical measures must be implemented in databases and server infrastructures:

• encryption to prevent unauthorized access by third parties;

• authentication mechanisms to restrict access rights to information systems;

• two-factor authentication (2FA) to limit unauthorized access without external devices;

• backup systems to ensure data recovery;

• active monitoring of access and usage logs.

All information systems and servers should undergo information security certification, with the possible application of international standards such as ISO/IEC 27001 and ISO/IEC 27701.

To protect personal data from various cyberattacks, it is necessary to deploy automated threat analysis systems, including antivirus software, firewalls, intrusion detection systems (IDS), Security Information and Event Management (SIEM) tools, as well as artificial intelligence-based real-time data analysis and filtering mechanisms within information databases.

The prevention of crimes involving the unlawful collection, processing, or dissemination of personal data cannot be ensured solely through legal measures, but also requires effective organizational and technical mechanisms. Key factors in this regard include interagency cooperation, oversight of responsible officials, personnel training, and the availability of a technological infrastructure aligned with information security standards. International experience demonstrates that genuine protection of personal data can be achieved only through the implementation of organizational and technical measures based on a comprehensive and integrated approach.

References

1. Abdurasulova, Q.R. Criminology. Textbook. Responsible editor: Doctor of Law, Professor M.H. Rustamboyev. – Tashkent: Publishing House of the Tashkent State Law Institute, 2008. 305 p.
2. Urazaliyev. M.Q. Science through time and space / - Society and innovations Issue - 1, N°02 (2020) / ISSN 2181-1415. 237 p.
3. Decree of the President of the Republic of Uzbekistan dated January 9, 2019, No. PF-5618, “On Fundamental Improvement of the System for Enhancing Legal Awareness and Legal Culture in Society.” National Database of Legislation of the Republic of Uzbekistan.https://lex.uz/ru/docs/4149765.
4. Senate Committee: In the past year alone, nearly 200 crimes were committed per 100,000 population in the republic.https://senat.uz/oz/events/post-3413
5. Abdurasulova, Q.R. Criminology. Textbook. Responsible editor: Doctor of Law, Professor M.H. Rustamboyev. – Tashkent: Publishing House of the Tashkent State Law Institute, 2008. p. 102.
6. https://www.consultant.ru/document/cons_doc_LAW_502182/
7. https://zakon.rada.gov.ua/laws/show/1089-20#Text;https://www.law.cornell.edu/cfr/text/47/64.1200; https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act
8. https://www.consultant.ru/document/cons_doc_LAW_34661/acf6fcbe94359c4ba136911fdad4b 570aa593e48/