International Journal of Business, Law and Political Science
Homepage : https://e-journal.antispublisher.id/index.php/IJBLPS
Email : admin@antispublisher.com

e-ISSN : 3032-1298
IJBLPS, Vol. 2, No. 8, August 2025
Page 292-302

Issues of Criminal Liability for Violation of Legislation on Personal Data in Some Foreign Countries Annotation

Choriev Anvar Kuzievich,
Independent Researcher at Tashkent State University of Law, Uzbekistan

DOI : https://doi.org/10.61796/ijblps.v2i8.345

Sections Info

Article history:
Submitted: April 11, 2025
Final Revised: May 16, 2025
Accepted: June 20, 2025
Published: July 06, 2025

Keywords:
Personal data
Violation of personal data legislation
Unlawful collection
Systematization
Storage
Modification
Completion
Use
Transfer
Dissemination
Destruction of personal data

ABSTRACT

Objective: *This article aims to analyze the criminal liability mechanisms for violations of personal data protection laws across several foreign jurisdictions, comparing them with the legal framework in Uzbekistan.* ***Method:*** *A comparative legal analysis was conducted, examining statutory regulations, case law, and institutional practices in countries such as Belarus, Kazakhstan, the United Kingdom, and Japan.* ***Results:*** *The findings indicate that while Belarus and Kazakhstan have criminal provisions similar to Uzbekistan's legal system, other countries adopt divergent approaches. For instance, the United Kingdom imposes criminal liability through the Data Protection Act 2018, while Japan emphasizes constitutional and administrative legal instruments without explicit criminal penalties. These disparities highlight the absence of a harmonized global standard for criminal liability in personal data protection.* ***Novelty:*** *This study provides a detailed comparative perspective on the diversity of legal mechanisms employed globally to address personal data violations and underscores the need for Uzbekistan to modernize and harmonize its criminal law framework in line with international best practices, without compromising its legislative sovereignty.*

INTRODUCTION

One of the key priorities in modern legal reform across many countries is the establishment of robust mechanisms to protect individual privacy and personal data. In this context, personal data legislation plays a critical role in safeguarding citizens' rights in the digital age. The increasing reliance on digital technologies and cross-border data exchange has made the issue of legal liability for the unlawful handling of personal data a global concern. This article explores the criminal liability for violations of personal data legislation in several foreign countries, offering a comparative legal analysis. The legal frameworks of nations such as Russia, Belarus, Kazakhstan, Ukraine, Germany, Denmark, the Netherlands, and Japan are examined to understand how different jurisdictions impose liability for unlawful data collection, storage, dissemination, or modification. The findings reveal a lack of a unified approach globally, with some countries incorporating criminal liability directly in their criminal codes, while others rely on specialized laws such as data protection acts. Furthermore, significant variations exist in the scope of protected data, the severity of penalties, and the requirement of intent or negligence for criminal liability. These differences underscore the complexities of

establishing international standards in personal data protection. The analysis also highlights that Uzbekistan's approach shares similarities with several CIS countries but can benefit from integrating international best practices. Ultimately, the comparative study underlines the importance of harmonizing data protection legislation with technological advancements and ensuring that criminal law serves as an effective deterrent against data-related offenses while upholding fundamental human rights[1].

RESEARCH METHOD

The methodology for this article is grounded in a comparative legal analysis aimed at examining the issues of criminal liability for violations of personal data legislation across several foreign jurisdictions. The research primarily utilized doctrinal legal research methods, including the study of legislative texts, legal doctrines, and relevant scholarly opinions. The author systematically analyzed the criminal codes and specialized laws of countries such as Russia, Belarus, Kazakhstan, Ukraine, Denmark, Germany, the Netherlands, Japan, the United Kingdom, France, and others. Legal provisions related to personal data protection were identified, categorized, and evaluated in terms of their scope, enforceability, and specific offenses covered. The study also included an interpretive approach, wherein legal norms were assessed based on their contextual application and alignment with international standards on data privacy. Secondary sources such as academic journals, legal commentaries, and policy documents further informed the assessment of legislative intent and practical enforcement challenges. Moreover, the research incorporated comparative techniques to highlight similarities and differences between legal systems, especially in how they treat intentional versus negligent violations, the identity of liable subjects, and the forms of criminal conduct recognized. This approach facilitated the identification of gaps and strengths in Uzbekistan's current legal framework relative to global practices. By contrasting Uzbekistan's legislative stance with that of other nations, the study provides valuable insights into potential improvements in criminal legal protection concerning personal data. Through this method, the author aims to contribute to the enhancement of domestic legal instruments and support more effective enforcement mechanisms for data protection laws[2].

RESULTS AND DISCUSSION

One of the most critical priorities of the current stage of democratic reforms in our country is the consistent implementation of a system for strengthening the rule of law and legality, ensuring reliable protection of human rights and interests, combating crime, and preventing criminal offenses[3].

According to the Decree of the President of the Republic of Uzbekistan No. PQ–3723 dated May 14, 2018, which approved the Concept for the Improvement of the Criminal and Criminal Procedure Legislation of the Republic of Uzbekistan, the tasks of improving criminal legislation and ensuring reliable protection of human rights and freedoms have been identified as key objectives[4].

At present, legal liability for violations of personal data legislation exists in almost all countries of the world.

E. Khokhlova identifies two general models of such liability. According to her, the first model provides for criminal liability for violations of rules on the processing and storage of personal data as reflected in the criminal legislation, while the second model enshrines this liability in special legislation.

We shall first examine the liability model enshrined in criminal legislation.

Due to the fact that the legislative development of the CIS member states shares a common legal heritage (originating from the former Soviet Union), issues related to criminal liability in all of these countries are regulated by their respective Criminal Codes[5].

The Criminal Code of the Russian Federation contains several provisions directly or indirectly related to the handling of personal data. In particular:

Article 137 establishes liability for the violation of the inviolability of private life;

Article 138 criminalizes breaches of the confidentiality of correspondence, telephone conversations, telegraphic or other communications;

Article 138.1 addresses the unlawful circulation of technical devices designed for the covert acquisition of information;

Article 155 sets out penalties for the disclosure of adoption secrets;

Article 183 establishes liability for the unlawful acquisition and disclosure of information constituting commercial, tax, or banking secrets;

Article 272.1 concerns the unlawful use and/or transmission, collection, and/or storage of computer information containing personal data, as well as the creation and/or maintenance of information resources intended for such unlawful use or dissemination;

Article 310 imposes liability for the disclosure of preliminary investigation data [6].

Although a separate Law "On Personal Data" was adopted in the Russian Federation on July 27, 2006, the criminal legislation does not establish a distinct provision imposing liability specifically for violations of this law. Instead, as discussed above, liability in relation to the handling of personal data is fragmented and distributed across various articles of the Criminal Code depending on the nature of the offense.

As noted by V.V. Vabishchevich, "The current wording of the provisions of the Criminal Code of the Republic of Belarus, adopted on May 9, 1999, relating to encroachments on personal data, has undergone no significant changes since the Code's adoption. At that time, the issue of information security for the individual, society, and the state was not as pressing, and the unlawful acquisition of personal data was not perceived as a serious socially dangerous act. This was largely due to the limited availability of sources for collecting personal data, as well as the underdevelopment of technologies enabling the theft and criminal exploitation of such information. However, the legislator did regulate the criminal-legal protection of certain types of information within a narrowly defined scope of permitted access and ensured corresponding safeguards" [7].

For instance, the Criminal Code of Belarus provides criminal liability for: the disclosure of adoption secrets , the violation of medical confidentiality , the unlawful disclosure of commercial secrets , breaches of the secrecy of voting, violations of the confidentiality of correspondence, telephone conversations, telegraphic or other messages , commercial espionag, intentional disclosure of state secrets , and intentional disclosure of official secrets .

At the same time, Article 203 of the Criminal Code of the Republic of Belarus establishes liability for unlawful acts concerning private life and personal data, while Article 203^2 provides for criminal liability for failure to comply with the requirements for the protection of personal data .

It is thus evident that, similar to the criminal legislation of Uzbekistan, the criminal law of the Republic of Belarus also envisages specific liability for violations involving personal data legislation[8].

In the Republic of Kazakhstan, the Law “On Personal Data and Their Protection” No. 94-V, dated May 21, 2013 was adopted, and following its adoption, corresponding amendments were introduced into Article 147 of the Criminal Code. This provision, titled “Violation of Privacy and of the Legislation of the Republic of Kazakhstan on Personal Data and Their Protection,” criminalizes the failure of persons responsible for ensuring the protection of personal data to take appropriate measures, provided that such failure causes significant harm to the rights and legitimate interests of individuals.

The concept of “significant harm” includes, inter alia, the violation of an individual’s constitutional rights and freedoms. Other criminally punishable acts under this provision include the unlawful collection and/or processing of personal data, where such actions cause substantial damage to the rights and legitimate interests of the data subject [9].

On 1 June 2010, Ukraine adopted the Law “On Personal Data,” thereby harmonizing its domestic legislation with European standards by signing the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol . Although a draft law was subsequently developed to introduce a number of amendments to the Criminal Code to ensure the implementation of this Law, the proposed changes envisaged criminal liability for the following acts:

the unlawful collection, registration, accumulation, storage, adaptation, alteration, updating, use, destruction or dissemination (including public disclosure, sale, or transfer to third parties) of confidential personal data, including dissemination via mass media or through public performances or publications, as well as transmission to third parties in violation of legal requirements;

the illegal dissemination or falsification of personal data, resulting from a failure to comply with statutory data protection obligations, where such violations cause significant harm to the individual;

the intentional provision of unauthorized access or transfer of personal data by the owner, user, or authorized person managing the personal data database to third parties

in breach of the law, resulting in unlawful dissemination or falsification of such data and significant harm to the data subject[10].

The draft legislation envisaged the inclusion of these acts as separate offences in new articles of the Criminal Code. However, due to a lack of political support, these proposed amendments were not incorporated into the Criminal Code.

Currently, Article 182 of the Criminal Code of Ukraine, titled "Violation of the Inviolability of Private Life," establishes criminal liability for the unlawful collection, storage, use, destruction, dissemination, or unauthorized modification of confidential information about an individual, provided such actions are not otherwise addressed under different provisions of the Code[11].

Under the first part of this article, such offenses are punishable by a fine ranging from 500 to 1,000 times the non-taxable minimum income, correctional labor for up to two years, probationary supervision for up to three years, or restriction of liberty for the same term.

The second part of Article 182 prescribes stricter liability if the offense is committed repeatedly or causes significant harm to rights, freedoms, and interests protected by law. In such cases, the punishment may include probationary supervision or restriction of liberty for a term of three to five years, or imprisonment for the same period[12].

For the purposes of this provision, "significant harm" is understood as material damage exceeding 100 times the non-taxable minimum income.

Importantly, the provision explicitly states that the public dissemination of information about criminal or other offenses – if done in compliance with the law – through mass media, journalists, public associations, or trade unions, shall not be regarded as an offense under this article and shall not give rise to criminal liability .

In Denmark, the Act No. 502 "On the Protection of Personal Data," adopted on 23 May 2018, is currently in force. However, the Criminal Code of the Kingdom of Denmark establishes liability for only a limited range of acts recognized as infringements upon the inviolability of personal data.

In this regard, particular attention should be paid to Section §264d of Chapter 27 of the Criminal Code, which is titled "Crimes Against Personal Honor and Certain Individual Rights." This section addresses the unlawful use of information and images relating to a person's private life and personal data. According to the provision, "a person who discloses information or images relating to another person's private life, or an image of another person, under circumstances where such content is presumed to have been concealed from the public, shall be held criminally liable."

Notably, Section §264d also applies to information and images related to deceased individuals. On the basis of this legislative approach, scholars such as L.A. Bukalerova and A.V. Ostroushko have proposed extending criminal liability to include the unauthorized use of visual representations of deceased persons .

Similarly, in the Kingdom of the Netherlands, Book 2, Title V of the Criminal Code — "Crimes Against Public Order" (Articles 138–139g) — protects the right to personal

data privacy not through constitutional status, but depending on the manner in which such a right has been violated. The legislature defines the unauthorized collection of personal data as a crime when such data is obtained through the use of technical means such as surveillance, eavesdropping, or recording devices.

Part 1 of Article 139a explicitly outlines the methods of data collection, stipulating that if conversations conducted in a residence, private room, or building are recorded using technical means without the consent of the participants and without being physically present during the conversation, such an act shall be deemed a criminal offense[13].

According to Part 2 of Article 139a, a person who, by means of technical equipment, listens to or records information while it is being transmitted to a third party – particularly when such transmission occurs within a dwelling or via a computer device or system – shall also be held criminally liable.

Article 139b of the Criminal Code provides for liability in cases similar to those described in Article 139a, with the distinction that the unlawful actions may occur not only in a residence but in any other location, provided they are carried out secretly and intentionally .

In the Criminal Code of the Federal Republic of Germany, Section 15 is entitled "Infringement of Privacy and Personal Secrets", which provides protection not only for the privacy of individuals (such as conversations, images, personal and commercial secrets), but also for technically protected information. The key criterion for protection is the absence of lawful access to such data.

In Germany, criminal legal protection of personal data is closely aligned with the European Union's stringent regulations on the processing of personal data. These rules define personal data broadly and emphasize the importance of legality throughout the entire data lifecycle—collection, storage, transmission, disclosure, and usage[14].

Criminal liability is established for unauthorized access to data, unlawful processing, retention of data, and the handling of devices specifically designed for such purposes. For instance, one category of crimes against personal life includes violation of the confidentiality of speech. Under §201, paragraph 1, a person commits an offense if, "without proper authorization," they record another person's non-public verbal communication using audio devices, use such recordings, or provide access to third parties.

Such actions are criminalized when they pose a potential harm to the legitimate interests of the individual.

Moreover, other crimes involving breach of the secrecy of communication include:

§201a – Violation of personal privacy through images, photographs, or videos;

§203 – Violation of personal secrets in the context of professional confidentiality, e.g., doctors, lawyers;

§§202–206 – Violation of secrecy of letters, telephone communications, or telecommunication transmissions;

§169 – Forgery of civil status documents.

The second group of crimes involves technical breaches of personal data protection, including:

§202a – Unauthorized access to data;

§202b – Interception of data;

§202c – Preparation for data espionage (e.g., developing, acquiring, selling, distributing, or providing software and codes intended for unauthorized access);

§202d – Data handling of stolen information, which criminalizes the purchase, dissemination, or public disclosure of unlawfully acquired data for commercial gain or to cause harm to others[15].

These provisions reflect Germany's commitment to criminalizing all forms of data-related privacy violations, aligning with international standards on personal data protection .

In accordance with Articles 13 and 35 of the Constitution of Japan, all citizens of the country are guaranteed the right to privacy, which includes the protection of personal data as an integral part of private life. This constitutional safeguard forms the legal basis for Japan's data protection regime .

The institution of personal data protection in Japan was legally established with the adoption of the Act on the Protection of Personal Information (APPI) in 2003, which came into force on April 1, 2005. The provisions of this law are aimed at protecting the confidentiality of information within the scope of personal life, including by means of criminal legal instruments where necessary.

Unlike some other jurisdictions, Japan's Criminal Code does not contain a separate provision specifically addressing personal data protection. That is, offenses in this sphere are not classified as distinct crimes in the Code[16].

Instead, Chapter 13 of the Criminal Code, entitled "Crimes Related to Breach of Secrets," provides general protection against intrusions into private life through two main offenses:

Article 133: Unlawful opening of correspondence;

Article 134: Unauthorized disclosure of professional secrets, applicable to doctors, attorneys, notaries, and other professionals who are legally obliged to maintain confidentiality.

Thus, while criminal liability for breaches of personal data protection is not independently regulated under Japanese criminal law, the right to informational privacy is nonetheless recognized and protected through a combination of constitutional provisions, administrative law (APPI), and selected criminal statutes related to secrecy and professional duties .

In certain jurisdictions, criminal liability for violations of personal data legislation is not enshrined in the general criminal codes but is instead embedded within specialized regulatory acts governing data protection. A clear example of this approach can be found in the United Kingdom, where, in the absence of a codified criminal law system, criminal sanctions for infringements of personal data rights are stipulated in the Data Protection Act 2018 (DPA). This Act replaced the earlier Data Protection Act 1998 and serves as the

main legislative framework for incorporating the provisions of the General Data Protection Regulation (GDPR) into domestic law [17].

According to the DPA 2018, every data controller or data processor is required to strictly comply with the data protection principles, which are fundamental to the lawful processing of personal data. On the basis of these principles, legal scholars generally classify criminal violations of personal data legislation into two categories:

The first category includes offenses related to unauthorized re-identification and the improper processing of anonymized data:

Re-identification without the data controller's consent;

Processing anonymized data in breach of lawful safeguards (Section 171 of the DPA);

Unlawful acquisition or re-identification of personal data under coercive or deceptive circumstances, such as:

during recruitment;

in the course of employment relationships (where the employer is liable);

within service provision contracts (where the contractor is liable);

or within public service delivery scenarios (Section 184 of the DPA).

The second category pertains to intentional or negligent misuse of personal data, including:

Obtaining, retaining, disclosing, or selling personal data without the consent of the data controller (Section 170 of the DPA);

Such actions are considered criminal if they result in, or are likely to result in, significant harm to the rights and freedoms of individuals;

Additionally, any action that involves altering, deleting, or concealing personal data in order to prevent a data subject from accessing their lawful information rights also constitutes a criminal offense under Section 170 [18].

This model demonstrates a regulatory-criminal hybrid approach to safeguarding personal information, wherein specific unlawful conduct within the data protection domain is punishable under sector-specific legislation, rather than through general criminal codes. Such an approach underscores the specialized nature of data protection offenses in jurisdictions like the UK, reflecting a shift toward precision-based legal regulation in the digital age .

In the criminal legislation of Spain, criminal liability is established for the unlawful collection (illegal interception) of electronic messages, files, and other telecommunication signals containing personal data that must be kept confidential, as well as for the unlawful disclosure of such data obtained by the data processor. In this regard, special attention is paid to personal data related to individuals' ideological and religious beliefs, health status, or sexual orientation. The very act of unlawfully collecting such data is considered a criminal offense, and if such actions are committed against minors or persons with disabilities for the purpose of gaining benefit, they are considered aggravating circumstances .

In some countries, the concept of "identity theft" exists, encompassing the unlawful appropriation of personal data with various intents. For example, in the United States, Canada, and Australia, such acts are committed to facilitate the commission of new crimes or to evade criminal liability. In France, such acts are regarded as breaches of peace, violations of honor and dignity; in Finland, they involve using another person's identity to cause harm or create obstacles .

In the Criminal Code of France, there exists a systematic classification of criminal offenses involving personal data as an object. These offenses are characterized by a high degree of detail. In particular, Chapter VI, entitled "Attacks Against Persons," outlines actions related to the violation of private life in the following sections:

Section I – Infringement of private life;

Section II – Violation of a person's image;

Section IV – Breach of confidentiality.

Offenses specifically related to personal data are set forth in the following sections:

Section V – Infringements upon individual rights (involving the maintenance of records and the processing of information);

Section VI – Situations involving the examination of a person's genetic characteristics or their identification through genetic markers .

Based on the comparative analysis of the experiences of foreign countries discussed above, the following conclusions can be drawn:

1. Unlike the criminal legislation of Uzbekistan, most foreign criminal laws rarely provide for specific liability for violations of legislation on personal data (only in Belarus and Kazakhstan are there dispositions comparable to the relevant provision in the Criminal Code of Uzbekistan);
2. In the majority of countries, criminal acts related to personal data are treated as part of offenses against the inviolability of private life, the secrecy of correspondence, or the confidentiality of other types of information;
3. There is no unified approach to defining the composition of offenses related to personal data in the dispositions of criminal statutes;
4. As for the subject of the offense, different approaches exist across jurisdictions: in some countries, the subject is a special entity, while in others, any individual or legal entity (such as data collection and processing operators) may be held liable;
5. While Uzbek law requires intentionality as a necessary element of this crime, in some countries, criminal liability may also arise in cases of negligent violations[19].

CONCLUSION

Fundamental Finding : This study demonstrates that while there is a universal recognition of personal data protection as a fundamental human right, the criminal liability frameworks addressing data violations vary significantly across jurisdictions, with only a few countries like Belarus and Kazakhstan incorporating explicit criminal

provisions similar to Uzbekistan. **Implication :** These findings suggest that Uzbekistan could enhance its legal system by adopting a more comprehensive and harmonized approach, aligning its criminal legislation with international standards while preserving its legal identity. **Limitation :** The analysis is primarily limited to selected countries and does not cover the full scope of enforcement practices or the effectiveness of criminal sanctions in deterring data violations. **Future Research :** Further studies should focus on the practical implementation of criminal liability in personal data protection, evaluating the enforcement mechanisms, prosecutorial trends, and the interplay between criminal, administrative, and civil remedies to provide a more holistic understanding of global data protection systems.

REFERENCES

[1] M. I. Savintseva, «Constitutional and legal problems of regulating informational relations in Japan: History and modernity», PhD Thesis, Moscow, 2007.

[2] «Criminal Code of the Federal Republic of Germany (Strafgesetzbuch – StGB)». https://crimescience.ru/wp-content/uploads-2021.pdf

[3] «Criminal Code of the Kingdom of the Netherlands (Wetboek van Strafrecht)». 2025 y. https://wetten.overheid.nl/BWBR0001854/2025-05-15

[4] «Criminal Code of the Republic of Belarus dated July 9, 1999 No. 275-Z (as amended as of 17.02.2025)». 2025 y. https://continent-online.com/Document/?doc_id=30414984#pos=6;-140

[5] «Criminal Code of the Republic of Kazakhstan No. 226-V dated July 3, 2014 (as amended as of May 19, 2025)». 2025 y.

[6] «Criminal Code of the Russian Federation No. 63-FZ of June 13, 1996 (as amended up to April 21, 2025, effective from May 2, 2025)». 2025 г. [Онлайн]. Доступно на: https://www.consultant.ru/document/cons_doc_LAW_10699/

[7] «Criminal Code of Ukraine No. 2341-III of April 5, 2001 (as amended as of January 9, 2025)». 2025 y. https://kodeksy.com.ua/ka/ugolovnyj_kodeks_ukraini/statja-182.htm

[8] E. V. Khokhlova, «Criminal law protection of personal data in foreign countries», *Bull. South-West State Univ. Ser. Hist. Law*, cc. 62–78, 2022, doi: 10.21869/2223-1501-2022-12-4-62-78.

[9] Yu. A. Govenko, *Criminal law protection of private secrets*. Pyatigorsk: RIA KMV, 2014.

[10] «Danish Criminal Code: English version». https://www.ojp.gov/ncjrs/virtual-library/abstracts/danish-criminal-code-english-version

[11] «Decree of the President of the Republic of Uzbekistan "On the Strategy 'Uzbekistan – 2030'"». 2023 y. https://lex.uz/uz/docs/-6600413

[12] V. V. Vabishchevich, «Foreign experience of criminal law protection of personal data», *J. Belarusian State Univ. Law*, cc. 72–80, 2019.

[13] «Law of the Republic of Kazakhstan "On Personal Data and Their Protection" No. 94-V dated May 21, 2013». 2013 y. https://adilet.zan.kz/rus/docs/Z1300000094#z421

[14] «Law of Ukraine "On the Protection of Personal Data" No. 2297-VI dated June 1, 2010». 2010 y. http://www.singlewindow.org/docs/57

[15] A. K. Zharova, «Legal regulation of personal data protection in the UK», *State Law*, cc. 70–78, 2017.

[16] A. Kh. Khuade, «Mechanism for ensuring the right to privacy in the Russian Federation», *Bull. Maykop State Technol. Univ.*, cc. 69–73, 2014.

[17] «Penal Code of Japan (刑法 Keihō)». https://sherloc.unodc.org/cld/uploads/res/document/jpn/1907/penal_code_html/Penal_Code_of_Japan.pdf

[18] «Presidential Decree of the Republic of Uzbekistan No. PQ–3723 dated May 14, 2018, "On the Concept for the Improvement of Criminal and Criminal Procedural Legislation of the Republic of Uzbekistan"». 2018 y.

[19] A. S. Ozerova, «Social conditionality of criminal law protection of personal data: experience of some foreign countries», *Leg. State Theory Pract.*, cc. 163–168, 2022.

*** Choriev Anvar Kuzievich (Corresponding Author)**
Independent Researcher at Tashkent State University of Law, Uzbekistan
E-mail: anvarkuziyevich@gmail.com