ORIGINAL ARTICLE

INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE

ISSN: 2692-5206, Impact Factor: 12,23

American Academic publishers, volume 05, issue 09,2025

Journal: https://www.academicpublishers.org/journals/index.php/ijai

VIOLATION OF THE INVIOLABILITY OF PERSONAL DATA IN THE DIGITAL WORLD: A NEW TYPE OF MODERN CRIME

Karamanova Benazir Karamanovna
Lecturer of the Faculty of Law of KSU
Kojabaeva Gulnur Bakhit kizi
3rd Year Student of the Faculty of law of KSU
gkojabaeva20@gmail.com

Abstract: This article examines the concept of personal data and the types of crimes committed during their use or those that may be committed in the future. In particular, cases of committing crimes using the capabilities of artificial intelligence, which is forming as a product of the digital age, and their consequences are analyzed. Liability measures established by current legislation for such offenses will also be considered.

Keywords: personal data, use, crime, digital technologies, foreign experience, artificial intelligence, law, liability

In the modern digital age, the rapid development of technologies allows storing and transmitting information about people's personal lives online. However, along with these opportunities, the issue of protecting people's personal data is becoming increasingly relevant. Such cases as the illegal collection, storage, dissemination, or disclosure of personal data through the Internet are manifested as modern crimes.

Today, as countries develop, the types of crimes are also increasing. With the development of digital technologies, artificial intelligence is gradually entering human life. Of course, this has its own advantages, but we cannot deny that it can be used for other purposes. This, in turn, creates a new form of committing the crime of violating the confidentiality of personal data. Now, to fully understand the issue discussed in this article, we need to have an understanding of personal data and its confidentiality. In this regard, Article 4 of the Law of the Republic of Uzbekistan "On Personal Data" defines it as "personal data - information recorded electronically, on paper and (or) on another tangible medium, relating to a specific individual or allowing its identification" [1]. That is, a set of information reflected in documents or similar papers related to the person themselves, through which it is possible to identify them. Personal information includes everything from our name and surname to our date of birth, residential address, phone number, passport number, and even our photo. Sometimes even the buttons we press on the internet and the websites we visit can be considered personal information. In the digital world, this information is collected through various websites, applications, and services. If they fall into the wrong hands, they can be defrauded, financially damaged, or their reputation tarnished. It would not be an exaggeration to mention the concept of artificial intelligence [2]. Artificial intelligence is the ability of artificial intelligence systems to demonstrate cognitive functions: learning, including from their own experience, adapting to given parameters, and performing tasks previously available only to humans (or higher animals). Article 141^2 of the Criminal Code of the Republic of Uzbekistan establishes liability for violation of legislation on personal data. Illegal collection, systematization, storage, modification, supplementation, use, transfer, dissemination, transmission, depersonalization, and destruction of personal data, as well as non-compliance with the requirements for the collection, systematization, and storage of personal data on technical means physically located in the territory of the Republic of Uzbekistan and in personal databases registered in the prescribed manner in the state register of personal databases during the processing of personal data of citizens of the Republic of Uzbekistan using information technologies, including the

ORIGINAL ARTICLE
INTERNATIONAL JOURNAL OF ARTIFICIAL INTELLIGENCE
ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 09,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

World Wide Web, committed after the application of administrative penalties for the same actions, - are punishable by a fine from one hundred to one hundred and fifty times the base calculation amount or deprivation of a certain right for up to three years or correctional labor for up to two years [3].

Through this article, we can understand that if someone illegally collects, stores, transfers, or disseminates citizens' personal data (such as full name, passport, place of residence, phone number, personal photos, etc.) - this is considered a crime. In particular, the processing of personal data of citizens of Uzbekistan on the Internet or through other information technologies should be carried out only legally, through specially registered databases and technical means located on the territory of Uzbekistan.

No one shall disclose or disclose anyone's personal information without their consent or legal grounds. This rule - that is, maintaining the confidentiality of data - is mandatory for the data owner (owner), the organization processing this data (operator), or any other person who has obtained permission to use this data. That is, if you have someone's personal information, you are absolutely prohibited from sharing or sharing it with others without that person's permission. This is stated in Article 28 of the Law “On Personal Data” [4].

Recent advancements in technology, particularly in artificial intelligence (AI), are fundamentally changing our way of life on a global scale. Such capabilities as making complex medical diagnoses using AI programs, automating production processes, and analyzing documents in the judicial and legal system are widely used in practice. At the same time, the negative aspects of AI technologies are also manifested. In particular, the number of cases of committing various crimes using artificial intelligence is increasing. It is precisely this problem that has presented many countries with the need to develop specific legal norms for crimes related to artificial intelligence. According to the publication "Standard," experts in the UK are advising users to exercise caution when exchanging personal information with artificial intelligence-based chatbots. Professor of Computer Science at Oxford University Michael Woodridge commented on this, noting that advanced language models like ChatGPT can perform user tasks with high accuracy. Nevertheless, he noted that these technologies could use previously provided data to serve other users in the future [5]. This creates a risk of disclosure of personal data. The National Human Rights Centre of the Republic of Uzbekistan announces this on its website.

M.Wuldridge also pays serious attention to the risks associated with chatbots. According to it, all information collected during interactions with users is stored. This data will be transmitted not only to systems of this generation, but also to future models of chatbots. Also, confidential or personal information accidentally sent by the user to the system will not be deleted in the future. This is considered an important problem from the point of view of information security. Permanent storage of data in the system can create various threats. Therefore, caution is emphasized when using chatbots [6].

Today, countries around the world have chosen different approaches in this area. Below we will discuss how some of them - the European Union, the USA, China, and Great Britain - regulate AI crimes [7]. The European Union is one of the most active countries in this area. A draft law called the “AI Act” developed by the EU Commission in 2021 divided artificial intelligence systems into four categories based on their level of risk: strictly prohibited, high-risk, limited-risk, and minimal-risk AI systems. For example, technologies such as mass surveillance systems or real-time facial recognition are categorized as strictly prohibited. This document assigns responsibility to manufacturers and service providers in accordance with the level of AI

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 09,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

risk. For high-risk AI systems, special certification, audit, and monitoring requirements are established. This is aimed at protecting the private life, rights and freedoms of citizens.

Although the United States has not yet adopted a single federal law, several states have developed separate legal norms for crimes related to AI. Also in 2022, a draft document known as the "AI Bill of Rights" was published. It includes the principles of digital security of citizens, the protection of personal data, and the fight against discriminatory systems based on AI [8]. The US Federal Trade Commission (FTC) is taking action in this regard, recognizing such actions as the misuse of artificial intelligence, the dissemination of false information (deepfake technology), and the use of unfair algorithms against individuals as illegal.

In China, however, the approach to artificial intelligence technologies is much stricter [9]. According to the Law “Regulation of Deep Synthesis Technologies” which entered into force in 2022, any content created using AI must be accurate and truthful. Otherwise, this is considered dissemination of false information and entails criminal liability. At the same time, it is strictly forbidden to collect or process users' personal data using AI without their consent. China has full government control over AI systems, which is aimed at ensuring information security.

In Great Britain, a “risk-based” approach is used to regulate AI technologies. The “AI Regulation White Paper” published in 2023, proposes adapting existing legislation rather than adopting new laws to regulate artificial intelligence. This country intends to identify the risks arising from AI technologies and combat them through existing legal means. At the same time, it is established that in the event of damage caused by AI, manufacturers and service providers may bear direct responsibility.

Thus, each country's approach to artificial intelligence is based on its own political system, information security policy, and human rights principles. While European countries emphasize regulating AI based on risk levels, the USA aims to protect human rights and consumers. While China has strengthened order and censorship, Great Britain is trying to regulate AI based on existing legislation. But their common goal is to ensure a balance between technological progress and human security and rights.

In the future, with the further development of artificial intelligence technologies, it is natural that the crimes that can be committed through them will also become more complicated. Therefore, the development of unified approaches and the establishment of interstate cooperation at the international level is becoming increasingly important. Therefore, considering it important to prevent the possible future consequences of this increasingly urgent issue, we put forward the following practical proposals: Firstly, the improvement of criminal law norms: The articles of the Criminal Code related to the violation of the constitutional rights of citizens should be revised based on clear, transparent, and legal mechanisms. In particular, it is advisable to amend a separate article or article for offenses committed using digital technologies. For example, I think that in order to protect people's personal data from the misappropriation of artificial intelligence, which is becoming increasingly globalized, it is necessary to introduce a separate article or additions to the article. Because artificial intelligence is now independently appropriating people's information, which in the future will lead to the penetration of information about people's private lives and will easily fall into the hands of criminals.

Secondly, ensuring control and public participation: Cases related to violations of citizens' rights should be under public control. It is necessary to create a legal basis for the active participation of citizens and the media in this sphere. Explanatory work should be carried out in the mass media to explain to the general public that the dissemination of information about another person or about the secrecy of his personal correspondence without his permission

ISSN: 2692-5206, Impact Factor: 12,23
American Academic publishers, volume 05, issue 09,2025
Journal: https://www.academicpublishers.org/journals/index.php/ijai

entails serious liability. We believe that this should be widely explained, especially among adolescents. Because they live in the age of new technologies, they want to use various internet sites and thereby unknowingly commit crimes or become victims of such crimes. Therefore, to protect the rights and freedoms enshrined in the constitution, everyone from the state to small public organizations must act.

In conclusion, the digital world is a world of opportunities. But along with these possibilities, there are also dangers that we must be cautious of. In the future, the interaction of the state, society, and each citizen will be of great importance for the reliable protection of people's digital identity. Because the inviolability of personal data is not only a legal category, but also a guarantee of human honor, dignity, and security. Therefore, maintaining a fair balance between technological progress and human rights is one of the most important tasks facing today's and future generations.

References

1. https://lex.uz/docs/-4396419 Law of the Republic of Uzbekistan 02.07.2019
2. Filipova I.A. Sun'iy intellektni huquqiy tartibga solish: Rus tilidan tarjima Z.O. Kuvandikov, mas'ul muharrir A.R. Axatov - Samarqand: Samarqand davlat universiteti, 2022. - 7 bet.
3. https://lex.uz/docs/-111453 Criminal Code of the Republic of Uzbekistan
4. https://lex.uz/docs/-4396419 Law of the Republic of Uzbekistan 02.07.2019
5. http://nhrc.uz/oz/news/m12336
6. https://kun.uz/news/2024/01/10/buyuk-britaniyalik-olimlar-chat-botlarning xavfliligi-haqida-ogohlantirdilar
7. European Commission. Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). – Brussels: European Commission, 2021. – 108 b. – URL: https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A52021PC0206
8. The White House. Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. – Washington: Office of Science and Technology Policy, 2022. – URL: https://www.whitehouse.gov/ostp/ai-bill-of-rights/
9. Cyberspace Administration of China. Provisions on the Administration of Deep Synthesis Internet Information Services. – Beijing, 2023. – URL: https://www.cac.gov.cn/2022-12/11/c_1672224711138025.htm
10. UK Government. A pro-innovation approach to AI regulation: policy paper. Department for Science, Innovation and Technology, 2023. https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach