

## Theoretical and Legal Analysis of the Concept of Inviolability of Personal Data

**Abdishukurov Izzatillo Eshborievich**

Assistant of judge of Termez district court in criminal cases

**Annotation:** This article consistently analyzes the inviolability of personal information, the consequences that may arise as a result of this violation, and the issue of liability. The relevance of this article is related to the growing information security that has emerged with the development and globalization of information technology around the world. Various statistics and legislation have been widely used to increase the accuracy of this data. Within the framework of the topic, targeted references were given to the opinions of foreign and national scientists, scientific works, research results, newspapers and magazines, legislation of foreign countries. Also, a creative approach with tables helped to reveal the essence of the article content in more depth. The importance of the security of personal data and the possibility of ensuring their inviolability, first of all, was covered in the context of the topic and the development of proposals for the protection of personal data.

**Keywords:** personal information, privacy of information, information, state secret, privacy, information, social network, information security.

### Introduction

As a result of the rapid growth of technology, it has created certain legal issues and problems. One of them is privacy of personal data. In today's advanced information technology era, every person uses a certain social network in their daily life. Despite the fact that social networks are convenient for people to share information, they are becoming a huge database of users' personal information. In such a situation, a person's information can be threatened or used for their own purposes. In these cases, privacy is important.

### Methodology

The purpose of this study is to investigate the theoretical and practical problems of personal data privacy. The main purpose of the study is to identify some of the problems that arise in the protection of personal data and to develop reforms that should be implemented to prevent them.

To achieve these goals, the author used several methods of scientific research, such as statistical analysis, sociological analysis, synthesis, comparative.

### Results And Discussion

First of all, if we focus on the concept of personal data, according to Chinese M. Park and S. Chailar, personal data includes information that can explain the identity of a certain person, such as names, addresses, and lifestyle [1]. R. Beckwith and S. According to Mainwarings, name, address, phone number, mother's maiden name, SSN, gender, medical history, insurance are also considered

personal information [2]. The personal information we use on any platform on the Internet, such as social media accounts or personal online banking accounts and other information, is our personal information [3].

The General Data Protection Regulation (GDPR), which entered into force for all EU member states on May 25, 2018, states that, in addition to data about a general person, because it has a higher level of protection, the most relevant person special categories of personal data (also known as sensitive personal data) should be taken into account. This data includes genetic, biometric and health data indicating genetic or ethnic origin, political opinions, religious or ideological beliefs or trade union membership, as well as personal data [4].

If we talk about personal data privacy, this is one of the first privacy rights. Inviolability of a person means the inherent right of every citizen recognized from birth [5]. Inviolability of personal data is considered one of the main constitutional rights of a person, and it is prohibited to collect, store, use and distribute information about a person's personal life without his consent. Sometimes it defines additional powers in the form of getting acquainted with the registered information about the person, using them, making corrections in case of inaccuracies. The secrecy of correspondence and other information exchange constitutes a separate constitutional right and is considered one of the guarantees of personal privacy [6].

As for the research and opinions of Uzbek scientists on this topic, Yu. Rahmatova, analyzing the legislation of foreign countries on information security, found that articles related to information security are scattered in a number of countries [7], H.P. Hasanov and O.P. Ahmedova emphasized the great role of cryptography in ensuring information security [8], A. Varisov that the development of criteria for evaluating the effectiveness of the security system in information systems, using them to evaluate the system and certification of these systems is considered one of the most important issues in the field of security [9], M. .A. Artikova stated that in order to prevent the risk of leakage of valuable information and to solve the current problems of ensuring security, first of all, it is necessary to develop an information security policy in organizations [10].

H.P. According to Hasanov and O.P. Ahmedova, since most of the tools aimed at ensuring information security are purchased from foreign countries, we should start production of information security tools in our country and create new technologies. The issues referred to in these opinions are defined in the Decision of the President of the Republic of Uzbekistan dated April 3, 2007 "On measures to organize cryptographic protection of information in the Republic of Uzbekistan" [11] №. PQ-614.

These scientists mainly focused on information security issues and did not touch on personal data privacy. Despite the extensive coverage of information security issues, these issues are broad in scope, and the protection of personal information is not covered....

As for the opinions of foreign scientists on this issue, M.A. Efremova and P.V. Agapov, one of the scientists who studied foreign experience in protecting information security, reviewed the legal system of a number of countries on privacy of personal data [12], Chinese H. Zou states that the violation of personal data harms the normal life and interests of citizens for their personal or property security [13], A. Bradley, Areheart, L.Jessica Roberts regarding the Genetic Information Nondiscrimination Act (GINA) and the violation or protection of employees' personal information

by employers [14], E.I.Juck conceptual aspects of information security, including the programmed and hardware tools of information security systems conducting research on the subject and considered information to be the most valuable object at the present time [15], B. Sierzputovsky spoke about the consequences of the 2007 cyber attack on Estonia and the increased data privacy of the world community after this event [16], N. Kshetri noted that data has a potential value that can be used by those who want to make additional income [17].

Privacy of personal data is protected by a number of regulatory legal documents. Including the right to personal privacy in Article 3 of the Universal Declaration of Human Rights, the right to personal honor and dignity defined in Article 12 [18], as well as Article 17 of the International Covenant on Civil and Political Rights (December 19, 1966). - in part 1 of the article "It is not allowed to arbitrarily or illegally interfere in the personal and family life of anyone, arbitrarily or illegally encroach on the privacy of his home or the privacy of his correspondence, and encroach on his dignity and honor" [19].

In recent years, great importance has been attached to the development of information security in the Republic of Uzbekistan. As a clear example of this, we can see the following legal documents. First of all, the Constitution of the Republic of Uzbekistan [20], Article 28 of the Law of the Republic of Uzbekistan "On Personal Information" No. O'RQ-547 states that "The owner and The requirement that the operator or other person authorized to use the personal data must comply with is the confidentiality of the personal data. The owner and operator and other persons authorized to use personal data must not disclose and distribute personal data to third parties without the consent of the subject" [21].

Violation of privacy of personal data shall be prosecuted under Article 462 [22] of the Code of Administrative Responsibility. If the administrative punishment is committed again in cases where it is committed again, it will be prosecuted based on Article 1411 [23] of the Criminal Code.

Although the above laws provide norms that serve to ensure the privacy of personal data, it is not specified what kind of data is personal data. In addition, the issue of illegal creation of personal data is not covered in the disposition part of the above codes. However, someone can create and illegally use the information of another person. An example of this is when someone opens webmoney for himself through someone else's passport.

If we examine the legislation of foreign countries regarding this issue, although the document on information security was adopted at the convention held in Budapest on November 23, 2001 [24], currently, in the international framework, the protection of information security by law, regulating crimes related to it, preventing these threats and there is no normative legal document fighting against it.

Comparative legal studies show that the legal system of foreign countries is characterized by the lack of a systematic approach to the protection of information security. However, in some countries the information is protected by law.

The right to privacy of communication or correspondence, mail, telegraph and other communications, which is part of the right to privacy, is also protected by foreign criminal law. However, there are differences in the legislation of countries in this regard. Belgian law defines breach of communications or telephone communications as a crime against public order. The

Spanish Penal Code does not provide any law regarding such breach of confidential information. The criminal law of the CIS countries on the prosecution of crimes against computer data is similar in many respects, and in most of them the model provisions of the Criminal Code of the CIS countries have been adopted, but some of them are changing.

Comparative analyzes have shown that the criminal laws of many foreign countries do not have a systematic approach to the criminal-legal protection of information security. However, in the legislation of some countries, the information protected by law is defined as a certain type. The analysis shows that only Polish criminal law has a systematic approach to legal protection of information security. In several other countries, systematic protection of various types of classified information can be observed. In many countries, it was found that the issues of criminalizing actions against information security are scattered in certain parts of the Criminal Code. We have to admit that today most of the personal data breaches happen on social networks. According to Forbes magazine, the WhatsApp social network has provided user information to the American FBI (Federal Bureau of Investigation) several times, and the number of frauds on Telegram has increased. Fraudsters are using Telegram bots to create fake pages for online hotel booking services, real estate rentals, and even travel search by registering fake accounts in their schemes. In addition to these, when the encryption of messages was introduced in Whatsapp, another function was introduced - the possibility of saving a backup copy of chats on a "cloud" server. According to Durov, this is actually a trap, which, despite the fact that it is encrypted, allows users' information to be made available to third parties.

If we talk about the statistics of crimes related to the violation of the right to privacy of personal data, according to 18 Chilling privacy statistics, 79 percent of Internet users around the world have completely lost control over their personal data. Since the implementation of the GDPR in Europe on May 25, 2018, significant fines have been imposed for violations of these laws. As of January 2021, Italy and Germany have the largest fines.

### **Conclusion**

If we conclude by examining the above cases, after studying the concept of personal data in a comprehensive way, the author's tariff on personal data was developed. Personal privacy is one of the basic rights of a person, and it was found that there are many cases of violating the rights of a person by stealing, destroying or changing it without his permission. These issues have been extensively studied throughout the article, and a group of authors on personal data privacy has been formed. National and foreign laws have been reviewed to ensure the privacy of personal information. In the course of these researches, it was found that in all countries, norms preventing violations of privacy of personal data are not given in Criminal or other laws.

Following the above research, the following proposals were developed in order to ensure the privacy of personal data in Uzbekistan:

Although the law "On personal data" has been developed in Uzbekistan, the concepts provided for in Article 4 of this law are supplemented by clearly specifying what personal data includes and their types, and the disposition of personal data in the Criminal and Administrative Responsibility Codes. It would be appropriate to add the sentence "illegally create". Among other

things, a new decision should be developed by the Plenum of the Supreme Court in order to strengthen additional measures to prevent these situations and ensure human rights.

In addition, it is necessary to establish by law the norm that servers storing personal data in Uzbekistan should be located only in Uzbekistan. Because personal information of citizens of Uzbekistan is on the servers of foreign countries, it makes it difficult to ensure their privacy. Because the information of the Person determines his identity and by changing it, his reputation and honor can be damaged.

### Bibliography

1. M.Park, S. Chai, The Value of Personal Information: An Exploratory Study for Types of Personal Information and Its Value, *Asia Pacific Journal of Information Systems* Vol. 28 No. 3 – 2018. – B. 155.
2. R. Beckwith va S. Mainvaring, Privacy: Personal Information, Threats, and Technologies, *IEEE Xplore*, – 2009. – B. 2.
3. The official website: Hogan injury law firm // <https://www.hoganinjury.com/cybersecuritysecuring-personal-information/>
4. The official website: GDPR // <https://gdpr-info.eu/issues/personal-data/>
5. National encyclopedia of Uzbekistan letter Sh – T.: – 2000-2005. - B.65.
6. R.A. Muhitdinov, Legal encyclopedia of Uzbekistan "Adolat", - Tashkent: - 2009. - B. 528
7. Yu. Rakhmatova, Analysis of legislation of foreign countries in ensuring information security // *ORIENSS*. 2021. #6.
8. H.P. Hasanov, O.P. Ahmedova, "Cryptographic means of ensuring information security" // - T.: Society and management, - 2015. Issue 2. - B. 46.
9. A. Varisov Ensuring the security of information resources in the electronic commerce system // – T.: Society and management, - 2015. Issue 1. - B. 88.
10. M.A. Artikova, "Information security: problems of "leakage" of information by illegal means" // - T.: Society and management, -2014. Number 2. - B. 45.
11. Decision PQ-614 "On measures to organize cryptographic protection of information in the Republic of Uzbekistan". National database of legal documents, 19.11.2018, No. 06/20/5578/0984.M.A. Efremova, P.V. Agapov Crimes against Information Security: International Legal Aspects of Fighting and Experience of Some States, "Journal of Internet Banking and Commerce", April 2016, vol. 21, no. S3
12. H. Zou. Protection of Personal Information Security in the Age of Big Data, 12th International Conference on Computational Intelligence and Security, 2016.
13. A. Bradley Areheart, Jessica L. Roberts, GINA, Big Data, and the Future of Employee Privacy, *The Yale Law Journal*. – 2019. – B. 710-783.
14. E.I. Juk. Conceptual basic information security // *Mashinostroenie and computer technology*. #04.– 2010. – B.35.Bartłomiej Sierżputowski, The data embassy under public international, "British of international and comparative law", – 2019. – B. 225-242.

15. Nir Kshetri, Big data's impact on privacy, security and consumer welfare, *Telecommunications Policy* 38(11), November 2014
16. The official website: United Nations Organization, Universal Declaration of Human Rights
17. (United Nations, Universal Declaration of Human Rights) 10.24.1948. Available at: <https://www.un.org/en/about-us/universal-declaration-of-humanrights>.
18. A.Kh. Saidov, Republic of Uzbekistan and international treaties on human rights - T.: Adolat, - 2002. - B. 61.
19. Constitution of the Republic of Uzbekistan / National database of legal documents, 09.02.2021, No. 03/21/671/0093“ Law on personal data / National database of legislative information, 04/21/2021, No. 03/21/683/0375.
20. Code of Administrative Responsibility of the Republic of Uzbekistan / National Database of Legislative Information, 17.09.2021, No. 03/21/716/0877.
21. Criminal Code of the Republic of Uzbekistan / National Database of Legislative Information, 05.10.2021, №. 03/21/719/0929.
22. Matsnev, N. Criminal Code of Belgium. St. Petersburg: Yuridicheskiy Tsentr Press, 2004.
23. Kuznetsova, N. & Reshetnikov, F. Criminal Code of Spain. Moscow: Zertsalo, 1998.
24. Model Criminal Code of the CIS Member States, Adopted by the Resolution of Interparliamentary Assembly of the CIS Member States, 1996.