CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
http://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 02 Issue: 10 | Oct 2021 ISSN: 2660-5309

Ensuring Information Security as a Guarantee of Human Rights

O'rinov Nodirbek Toxirjonovich
Teacher, Department of Information Technology, Andijan State University
Ahmedov Husanboy Muhammadshukur o'g'li, Mirabdullayev Izzatillo Isroiljon o'g'li
Student, Computer science teaching methods, Andijan State University

Abstract:

The article is devoted to the actual problem of information security and the rights ratio brow century. In Uzbekistan, the concept of "information security", as a rule, is revealed through "the state of protection of the vital interests of the individual, society and the state." In the US and the European Union, the definition of "information security" associated with the legal principles of confidentiality, integrity and availability of information and information si tems. Implementation of these principles allows to balance the interests of various participative Cove legal relations, thus acting as a guarantee of human rights. The influence of modern technology is manifested primarily in the field of personal rights, among which the right to privacy occupies a special place. On the one hand, measures directly aimed at protecting this right act as guarantees of the right to privacy. On the other hand, when limiting the right to privacy, appropriate safeguards should prevent possible abuse. In addition to the principles of confidentiality, integrity and accessibility, specific legal principles have been developed to protect the right to privacy. The main mechanisms for protecting the right to privacy that are foundexpression in these principles are the consent of the personal data subject to the processing of personal data and his notification of such processing. At the same time, with the development of Internet technologies, these mechanisms turn out to be insufficient to respect the human right to privacy.

ARTICLEINFO

Article history:
Received 30 Aug 2021
Revised form 22 Sep 2021
Accepted 26 Oct 2021

Keywords: human rights, information security, legal principles, limitation of rights, security threats, privacy.

---***---

The development of guarantees of this right is carried out by creating additional mechanisms for protecting confidentiality, which are expressed in the presentation of specific requirements in the field of collection and processing of personal information. The improvement of technologies also leads to the emergence of new

threats to national security and information security of the state as one of its components. The need to protect them becomes the basis for limiting the right to privacy. The proportionality of restrictions to the purposes of their establishment is a guarantee of human rights and information security of the individual. In countries with democratic legal regimes tend to mouth Credited priority rights to ensure national security.

Human rights are the foundation of a modern rule of law. At the post-industrial stage of development, the protection of human rights takes on a special character. Improvements in information and communication technologies are accompanied by increased opportunities for their unfair use, which poses threats to information security and can lead to violations of human rights. In this regard, the problem arises of the relationship between information security and human rights, first of all, the right to privacy , the study of which is the subject of this article.

In Uzbekistan, the concepts of “security”, “information security” and “national security” are revealed through “the state of protection of the vital interests of the individual, society and states. Information security in this case is defined as the state of protection of national interests in the Republic of Uzbekistan in the information sphere, which consists of a set of balanced interests of the individual, society and the state, from internal and external threats. Legal doctrine generally follows these provisions.

In the domestic legal literature, the definition of "information security" is also used through the state of security of the information sphere, in which it is impossible to implement known threats in relation to its constituent elements. In this case, the concept of "information security" is considered as a more general category in relation to the concept of "information security", in which the emphasis is on a set of measures and actions aimed at ensuring the security of information. In this case, we are talking about the state of protection of information, and not the interests of the individual, society and the state.

In legal doctrine, the United States and the European Union's definition of "information without danger" is carried out through the transfer of specific elements of the information sphere, on the protection of which it is directed, and is associated with the legal principles con confidentiality, integrity and availability of information and information systems.

The implementation of these principles allows ensuring a balance of interests of various participants in legal relations, thus acting as a guarantee of human rights in the field of information security.

Subject to the principle of confidentiality, familiarization with confidential information, its processing and presentation of a request for its provision are allowed only for a person who has the right to access such information. The role of the confidentiality principle is to prevent harm that can be caused to public relations as a result of the unlawful provision and dissemination of information kept secret due to its importance for the safety of an individual, society or state. This principle corresponds to a kind of right to "conceal" information, ie. keep it secret, restrict third party access to it, control its intended use.

In contrast to confidentiality, ensuring the integrity of information has become relevant in the process of development of computer technologies and the emergence of opportunities for unauthorized access to information in order to amend or destroy it. A person who has information or the right to access information has the right to demand that its integrity be ensured, as well as, in some cases, the integrity of the information carrier, i.e. keeping them in their original, unchanged form, ensuring non-interference in the structure (form) and content of information. This principle is aimed at ensuring the authenticity of information, which allows the participants in public relations to maintain the necessary level of trust and confidence that they are dealing with the original information and its source, and not with falsification or modification.

The principle of accessibility plays an important role in the formation of guarantees of the human right to access information. This principle is intended to prevent restrictions and the creation of conditions for access

to socially significant information, especially in the interaction of man with the bodies of power, as well as to other information of which he has the right to demand. This principle lies at the basis of the implementation of measures on the access to information about the activities of state bodies and local authorities, environmental information, including by posting the information on the official websites of agencies and organizations.

The influence of modern information and communication technologies is manifested primarily in the field of personal rights, among which the right to privacy occupies a special place. We must agree with the statement that "without information security, there can be no privacy." Therefore, ensuring the information security of a person is the basis for legal protection of privacy. With the development of technologies, the volumes and speed of information exchange are significantly increasing, the range of possible ways of collecting, processing, providing and distributing it is expanding. As a result, the harm that can be caused to an individual through the disclosure of certain information or in connection with keeping it secret also increases. These processes are deepening contradictions, which are caused by the opposition of principles confit dentsialnosti and access rights to keep information confidential and the right of access to such information. Such contradictions arise both in private law and in public law relations.

In private law relations, the corresponding contradictions are expressed in the fact that in order to support freedom of expression, freedom of contract and entrepreneurial activity in the context of automation of business processes, the introduction of computer and Internet services, it is necessary to expand the possibilities of access to personal information and its subsequent use for commercial and other organizations. At the same time, the growth of adverse consequences for the individual in connection with such use of personal information requires restricting access to it by third parties, monitoring its use and creating additional mechanisms to protect the right to privacy.

In public law relations, specialized state information systems are increasingly used, for the full functioning of which it is necessary to expand the powers of the authorities in the field of processing various types of personal information in an automated mode. These processes, together with the measures that are being taken to ensure national security, lead to the formation of legislative restrictions on the right to the inviolability of private life. At the same time, the prevention of illegal interference in private life and abuse by the authorities is becoming one of the priority areas for ensuring the information security of an individual.

On the one hand, information security measures directly aimed at protecting this right act as guarantees of the right to privacy. At the same time, the development of appropriate measures is carried out by concretizing the legal principles of confidentiality, integrity and accessibility, taking into account the essence of the right to privacy and its possible violations.

On the other hand, when establishing restrictions on the right to privacy, appropriate safeguards should prevent possible abuse of such restrictions, leading to threats to the information security of the individual. As rightly noted in the domestic legal doctrine, “the panacea for such abuses ... is the principle of proportionality and the formula derived from it about the prohibition of excessive restrictions. This prohibition (in the process of legislative and law enforcement activity) means that restrictions permissible under the Constitution and international documents on human rights must correspond in content and scope to the objectives of the restrictions imposed and can only be applied to protect other equivalent legal values”.

In addition to the principles of confidentiality, integrity and accessibility, the legal doctrine has developed special legal principles for protecting the right to privacy, which determine the limits and conditions for the exercise of this right. In connection with the principle of confidentiality, such special legal principles determine the possibility of collecting personal data only by legal and good faith means and for specifically defined purposes, subject to prior notification or consent of the subject of personal data, ensuring their protection from such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. Along with the principle of integrity, the principle is applied, subject to which personal data must

correspond to the purposes of their use and, in accordance with such purposes, must be accurate, complete and up-to-date. The principle of accessibility is supplemented by principles that create conditions for the subject of personal data to access information about the operator's and the nature of the personal data of such a subject being processed, the main purposes of their use, the identity and location of the data operator, and also endow the subjects of personal data with additional rights, including the ability to destroy, correct, supplement or change your personal data. These principles are currently reflected in both national and international law.

The main mechanisms for protecting the right to privacy, which are expressed in the relevant legal principles, are the consent of the personal data subject to the processing of personal data and his notification of such processing. At the same time, the confidentiality of personal information is ensured by providing access or the ability to collect and process such information only to those persons who have received the appropriate consent of its owner. If before the stupas and the possibility of collecting and processing provided by law, it is mandatory notification of personal data processing of their owner. Notification is also mandatory in other cases determined by the subject of personal data or established by law, for example, in case of violation of the confidentiality or integrity of personal data. These mechanisms provide the subject of personal data with legal opportunities to control their use and, accordingly, guarantees the inviolability of his private life.

At the same time, with the development of the network internet and internet services, the creation of massive collections of information (known as "Big Data") and the development of cloud those nologies these mechanisms are not sufficient to comply with the rights chelove- ka on the inviolability of private life. In fact, the user is gradually losing control over the use of his personal data. So, when using cloud technologies, the process of transferring and processing data becomes indefinite for the user and, in practice, may consist in crushing information and placing it on servers located in various national jurisdictions.

In addition, the majority of users give their consent to the processing of their personal data without properly reading its terms and conditions, without understanding the legal consequences of such consent and without anticipating the subsequent use of their personal information. As a result, the mechanism for obtaining the user's consent to the processing of his personal information becomes a weak, in fact, formal guarantee that does not ensure the confidentiality of personal information and real protection of the right to privacy .

For modern e-commerce, prior consent and subsequent notification of the subject of personal data, as well as legal restrictions on the use of cloud technologies, create obstacles to business development and innovation. In this regard, restrictions on freedom of entrepreneurial activity on the Internet, caused by the use of traditional mechanisms to protect the right to inviolability of private life, become redundant.

The development of guarantees of this right is carried out by creating additional mechanisms for protecting confidentiality in relation to the consent of the subject of personal data and his notification , which are expressed in the presentation of specific requirements to persons who collect and process personal information. Such requirements may include establishing a special legal regime for so-called sensitive data, limiting the collection of certain personal information in digital form, including geolocation and biometric data, limiting the automatic adoption of legally significant decisions. A form of legal protection of personal data is also the restriction of their transfer to national jurisdictions, where the necessary guarantees of the right to privacy are not provided. At the same time, the requirements for the technical protection of personal data are increasing in order to prevent unauthorized access to data, to eliminate the consequences of their disclosure or compromise.

In the European Union, the right to privacy is considered a fundamental right. His protection is guaranteed by Art. 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter - the 1950 Convention) and the constitutions of the EU member states. Full control of the priority of the individual over his personal data to the traditional democratic freedoms (freedom of

entrepreneurship and freedom of speech) is the basis of several generations of national legislation in the sphere of protection of the inviolability of private life, normative legal acts of the EU and the decisions of the European Court of Human Rights.

In contrast, from the EU to the US, where in the lower level appears paternalistic function of the state, special requirements in the processing of personal data established only in the most sensitive areas. In other areas, the state gives priority to self-regulation, which is based on freedom of entrepreneurial activity, freedom of contract, freedom of speech and press. The state influences public relations by issuing various kinds of recommendations and political statements.

Despite the differences between the above approaches, it should also be noted that they tend to converge. Thus, in the EU, the Data Protection Directive 95/46 / EC prohibits the transfer of personal data of resident users to states outside the European Economic Community. An exception is “the transfer of personal data to third countries that provide an adequate level of protection”. It is recognized that such protection is provided in the United States, although there are exceptions. Thus, the transfer of personal data from the EU to the United States is allowed only if the operator is a member of the Safe Harbor Agreement or has agreed to other contractual terms that have been established to ensure adequate protection of personal data.

The development of technology leads to the emergence of threats to national security and information security of the state as one of its components. Neobhopersonalnymi data over traditional democratic freedoms (freedom of entrepreneurship and freedom of speech) is the basis of several generations of national legislation in the sphere of protection of the inviolability of private life, normative legal acts of the EU and the decisions of the European Court of Human Rights.

In contrast, from the EU to the US, where in the lower level appears paternalistic function of the state, special requirements in the processing of personal data established only in the most sensitive areas. In other areas, the state gives priority to self-regulation, which is based on freedom of entrepreneurial activity, freedom of contract, freedom of speech and press. The state influences public relations by issuing various kinds of recommendations and political statements.

Despite the differences between the above approaches, it should also be noted that they tend to converge. Thus, in the EU, the Data Protection Directive 95/46 / EC prohibits the transfer of personal data of resident users to states outside the European Economic Community. An exception is “the transfer of personal data to third countries that provide an adequate level of protection”. It is recognized that such protection is provided in the United States, although there are exceptions. Thus, the transfer of personal data from the EU to the United States is allowed only if the operator is a member of the Safe Harbor Agreement or has agreed to other contractual terms that have been established to ensure adequate protection of personal data.

The development of technology leads to the emergence of threats to national security and information security of the state as one of its components. Neobhoono is over. In the process of supervision, the values of a democratic society must be observed as conscientiously as possible ... ”.

The smaller the value of democratic values in the political regime, the b of the greater role played by national security for the preservation of the existing order of government, resulting in the establishment of various human rights restrictions, including the right to privacy. According to the position of the European Court of Human Rights expressed in the case

“Class and Others v. Germany”, “the right of secret surveillance of citizens, which is characteristic of a police state, is tolerated under the Convention only when it is strictly necessary for the preservation of democratic institutions”; states "may not, in the name of the fight against espionage and terrorism, take whatever action they deem appropriate."

Thus, in the context of the development of technologies, ensuring information security is one of the most important guarantees of human rights. Such guarantees are based on the observance of the principles of

confidentiality, integrity and availability of information and information systems. To ensure information security of an individual, special legal principles are being developed to protect the right to privacy, as well as additional mechanisms for its protection associated with the establishment of specific requirements in the field of collection and processing of personal information. In ensuring the national security and information security of the state, one of its components is the most important guarantees of human rights, the observance of the principle of proportionality when limiting them is. The implementation of these principles and mechanisms for protecting human rights while ensuring information security can take various forms, which depend on legal traditions and the political regime of the state.

Bibliography

1. V.N. Lopatin Information security of Russia: dis ... Doctor of Law. sciences. M., 2003.433 p.
2. Polyakova T.A. Legal support of information security in building the information society in Russia: dis ... Dr. jurid. sciences. M., 2008.437 p.
3. Human rights: textbook for universities / otv. ed. E.A. Lukashev. M .: NORMA, 2001.573 p.
4. Sokolov M.S. Information security. On the question of the content of the concept of "information security" // Zakon i pravo. 2011. No. 5. P. 9–14.
5. Streltsov A.A. Theoretical and methodological foundations of legal support of information security in Russia: dis ... Doctor of Law. sciences. Moscow: RSL, 2005.371 p.
6. Shvetsova T.V. Information security, information security, information protection: the relationship of concepts // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia. 2007. No. 2. P. 43–45.
7. Cumbley R., Church P. Is "Big Data" Creepy? // Computer Law and Security Review. 2013. No. 29. P. 601-609.
8. Coudert F. When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies // Computer Law and Security Review. 2010. No. 26. P. 377–384.
9. Crounse S. The Fair Information Principles: A Comparison of US and Canadian Privacy Policy as Applied to the Private Sector. NY: Rochester Institute of Technology, UMI Dissertations Publishing, 2009.174 p.
10. Grama J. Legal Issues in Information Security. Sudbury: Jones and Bartlett Publishers, 2010.526 p.
11. Goncalves ME, Jesus IA Security policies and the weakening of personal data protection in the European Union // Computer Law and Security Review. 2013. No. 29. P. 255–263.
12. Information Security and Privacy: a Practical Guide for Global Executives, Lawyers and Technologists.
13. T. Shaw, ed. Chicago: American Bar Association, 2011. 395 p.
14. King NJ, Raja VT Protecting the Privacy and Security of Sensitive Customer Data in the Cloud // Computer Law and Security Review. 2012. No. 28. P. 308–319.
15. McDonald AM, Cranor LF The Cost of Reading Privacy Policies // Journal of Law and Policy for the Information Society. 2008. Vol. 4. P. 540-565.
16. Ryan P., Falvey S. Trust in the Clouds // Computer Law and Security Review. 2012. No. 28. P. 513–521.
17. Silver D. National Security and Transparency: The Legal Frameworks and Factors Federal Courts Use to Balance Competing Democratic Values. PhD Diss. Chapel Hill, 2009.313 p.