TEXNİKA ELMLƏRİ

TECHNICAL SCIENCES

https://doi.org/10.36719/2663-4619/111/190-193

Rahim Rahimli
Khazar University
https://orcid.org/0009-0005-2061-6093
UOT 005:004
rehim4028@gmail.com

Ensuring the Protection of Personal Data As an Element of Information Security

Abstract

The article considers the legal regulation of personal data protection as an important element of information security, highlighting its critical importance in the modern digital landscape. The study examines the relevance of addressing the challenges associated with safeguarding personal data, presenting examples of emerging threats that have exacerbated the risks of data leakage. It identifies key measures, including legal frameworks, technological solutions, and organizational strategies, that contribute to strengthening the protection of personal data. Additionally, the article discusses the broader implications for organizations and individuals, emphasizing the necessity of proactive approaches to mitigate risks and enhance information security.

Keywords: *information security, personal data protection, protection, information, legal regulation*

Rəhim Rəhimli
Xəzər Universiteti
https://orcid.org/0009-0005-2061-6093
UOT 005:004
rehim4028@gmail.com

İnformasiya təhlükəsizliyinin unesenti kimi şəxsi məlumatların mühafizəsinin təmin edilməsi

Xülasə

Məqalədə fərdi məlumatların mühafizəsinin hüquqi tənzimlənməsi informasiya təhlükəsizliyinin mühüm elementi kimi nəzərdən keçirilir, onun müasir rəqəmsal mənzərədə kritik əhəmiyyəti vurğulanır. Tədqiqat şəxsi məlumatların qorunmasının gücləndirilməsinə töhfə verən hüquqi bazalar, texnoloji həllər və təşkilati strategiyalar da daxil olmaqla əsas tədbirləri müəyyən edir. Bundan əlavə, məqalədə risklərin azaldılması və informasiya təhlükəsizliyinin artırılması üçün proaktiv yanaşmaların zəruriliyi vurğulanaraq təşkilatlar və fərdlər üçün daha geniş təsirlər müzakirə edilir.

Açar sözlər: *informasiya təhlükəsizliyi, fərdi məlumatların mühafizəsi, mühafizə, məlumat, hüquqi tənzimləmə*

Introduction

Digital development is an undisputed catalyst for global progress. At the same time, global digitalization, the Internet, mobile communications, computer technologies, and the possibilities of scientific and technical achievements in this area inevitably give rise to risks and threats.

Ensuring information security and protecting personal data has recently become one of the key tasks not only on a global scale, but also within any state and organization.

At the international level, the mechanism for protecting personal data is reflected in the principle of privacy. The corresponding principle is contained in the International Covenant on Civil and Political Rights, which establishes that no one shall be subjected to arbitrary or unlawful interference with the inviolability of his home or the privacy of his correspondence, or to unlawful attacks on his honor and reputation (International Covenant on Civil and Political Rights).

Research

There are two main approaches to defining personal data in foreign legislation. Firstly, in some countries, personal data are identified with any information related to a given person (the Netherlands, Sweden, New Zealand, etc.). Secondly, some countries are characterized by detailing, establishing certain criteria for classifying information into a specified category (Great Britain, etc.). At the same time, the optimal regulation option is considered to be the presence of a carefully verified and legally secured balance of two basic information rights and freedoms: the right to access information affecting the interests of a person, and the right to restrict third parties' access to information about themselves (Dvoretsky & Chernyshova, 2007, pp. 12-13).

The European Union has developed and adopted provisions governing the protection of personal data, enshrined in the GDPR (General Data Protection Regulation). In accordance with this document, the rights of personal data subjects have been significantly expanded, while the obligations of operators and fines for failure to comply have increased significantly. The definition of personal data in the GDPR itself has the following content: "any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, surname, identification number, location data, online identifier or to one or more physical, physiological, genetic, mental, economic, cultural or social identity factors specific to that person."

At the same time, the leakage of personal data remains at a high level (Regulation (EU) 2016/679 of the European parliament and of the council, 2016).

At the same time, the problem is exacerbated by the emergence of modern challenges.

As an example of the emerging threat of a breach of personal data security, the following can be noted.

During the spread of the new coronavirus infection COVID-19, global changes occurred in the public life of people. Thus, many employers, in order to maintain the stability of their activities, were forced to transfer employees to a remote work mode, educational institutions organized distance learning opportunities, etc. Such specifics of work require strengthening information security in terms of protecting personal data, which presupposes the availability of reliable communication channels and sufficient material resources for the transition process (Data Protection and Privacy in the Digital Age. Research paper discussing global trends in personal data protection, 2021; OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Framework for protecting privacy, 2013).

The blurring of boundaries between corporate and personal devices, corporate and personal data, due to the fact that many employees work from home on their personal laptops and computers, a priori reduces the level of information protection (General Data Protection Regulation (GDPR) Overview. European Union's regulation on data protection and privacy, 2016).

At the same time, almost all organizations have encountered attempts to "leak" information during the period of remote work – both intentional (collusion of employees with attackers) and unintentional. For example, there were cases when employees received a mailing allegedly from the HR department of their company with information about dismissal in connection with the decision of the manager to optimize the staff in difficult pandemic conditions, and they were offered to find out more detailed information in an infected file attached to the letter or by clicking on a link to a site that steals personal data. Both the employees themselves, whose personal data was leaked to third parties, and the companies that received local and network infections in this way suffered damage

from such mailings (ISO/IEC 27001: Information Security Management. International standard for managing information security, 2013).

Ensuring the protection of personal data should be a priority task and contain measures to prevent their theft.

A successful solution to these problems is impossible without the use of a set of means and methods for protecting information.

Among the main areas of information protection, one can name organizational, legal and engineering-technical. At the same time, organizational information protection among these areas is given a special place (The Impact of COVID-19 on Cybersecurity and Data Protection. Examines changes in personal data protection during the pandemic, 2021).

Organizational information protection is designed to implement in practice the measures planned by the enterprise management to protect information through the selection of specific forces and means, including legal and engineering-technical ones. These measures are taken depending on the specific situation at the enterprise associated with the presence of possible threats affecting the protected information and leading to its leakage (ENISA Threat Landscape Report. European Union Agency for Cybersecurity's annual report on cybersecurity threats, 2023).

The key place in the technology of protecting the personal data of employees is the development of the regulation. The regulation on the protection of the personal data of the employee is the main document regulating the algorithm for protecting the personal data of the employee at a specific enterprise. This document occupies the main place in the information protection system of the enterprise. As a rule, the regulation determines the procedure for receiving, processing, storing, transferring and any other use of the personal data of the employee, as well as maintaining his personal file in accordance with the labor legislation of Azerbaijan (NIST Special Publication 800-53: Security and Privacy Controls. U.S. National Institute of Standards and Technology's guidelines for securing information systems, 2020).

One of the main problems for specialists who are operators of personal data before starting to collect and process such information is, first of all, the lack of a clear list of organizational and administrative documents necessary to confirm their compliance with the requirements of legislation in the field of personal data protection. A large number of responsibilities imposed on the operator of personal data by federal laws and acts lead to the need for documentary confirmation of compliance with all these requirements. If there is no understanding of the final list of documents, the specialist who is engaged in their development spends a lot of extra time writing documents that partially repeat each other, accordingly, there is a loss of efficiency of the specialist's work (Verizon 2023 Data Breach Investigations Report. Comprehensive report on cybersecurity incidents and trends, 2023).

In order to reduce the labor costs of a specialist in developing organizational and administrative documentation, it will be relevant to automate this process, which in the future will not only optimize the work, but also reduce the number of errors associated with the human factor, and reduce the financial costs of developing documents by specialized companies. Comparison of potential costs associated with the implementation of modern information technologies with the damage that can be caused by information leakage indicates that ensuring information security requires the investment of serious financial resources. In this regard, the formation of an expense item sufficient to finance information security should be one of the priority tasks of companies (Personal Data Protection Laws: A Comparative Study. Provides an overview of global regulations, 2020).

Conclusion

At the same time, it is important for citizens themselves to observe “digital hygiene” when using the Internet and technical devices, which ensures the minimization of the risks of theft of personal data: do not leave information about yourself, do not launch links, do not open files, that is, by default, consider that every incoming communication is communication from intruders. Perhaps it makes sense to think about the advisability of including in the educational program a subject in which students will study the basic aspects and means of ensuring the protection of their own personal data

(possibly both as a main subject and an optional circle). However, raising literacy on the issue of information security must be carried out for all age groups.

References

1. Dvoretsky, A. V., & Chernyshova, I. V. (2007). *Protection of personal data of employees under the legislation of foreign countries: bulletin Center for Comparative Labor Law*, 22. ISBN 5751119223, 12-13.
2. *Data Protection and Privacy in the Digital Age. Research paper discussing global trends in personal data protection.* (2021). https://www.sciencedirect.com/science/article/pii/S0267364921000933
3. *ENISA Threat Landscape Report. European Union Agency for Cybersecurity's annual report on cybersecurity threats*. (2023). https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat landscape
4. *General Data Protection Regulation (GDPR) Overview. European Union's regulation on data protection and privacy*. (2016). https://gdpr-info.eu/
5. *International Covenant on Civil and Political Rights, adopted by General Assembly resolution 2200 A* (XXI) of. (1966, December 16). https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (accessed 15.04.2021)
6. *ISO/IEC 27001: Information Security Management. International standard for managing information security* (2013, revised in 2022). https://www.iso.org/isoiec-27001-information-security.html
7. *NIST Special Publication 800-53: Security and Privacy Controls. U.S. National Institute of Standards and Technology's guidelines for securing information systems*. (2020). https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
8. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Framework for protecting privacy*. (2013). https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
9. *Personal Data Protection Laws: A Comparative Study. Provides an overview of global regulations*. (2020). https://link.springer.com/chapter/10.1007/978-3-030-30516-0_12
10. *Regulation (EU) 2016/679 of the European parliament and of the council. "On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 / EC* (General Data Protection Regulation) of 27 April 2016. https://ogdpr.eu/ru/gdpr-2016-679 (accessed 15.04.2021).
11. *The Impact of COVID-19 on Cybersecurity and Data Protection. Examines changes in personal data protection during the pandemic.* (2021). https://www.frontiersin.org/articles/10.3389/fcomp.2021.644678/full
12. *Verizon 2023 Data Breach Investigations Report. Comprehensive report on cybersecurity incidents and trends*. (2023). https://www.verizon.com/business/resources/reports/dbir/

Received: 13.08.2024
Revised: 24.10.2024
Accepted: 10.12.2024
Published: 22.02.2025