JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Legal Basis of Cybersecurity at the International and National Level

Boburjon T.Shokirov
Fergana State University 2nd year student of jurisprudence

Annotation: The legal framework for cybersecurity at the international and national levels has become a relevant topic with the rapid development of modern information technologies. Effectively combating cybercrime, protecting personal data, and ensuring the security of state systems are among the main goals of cybersecurity. At the international level, the Budapest Convention is recognized as the main regulatory document for strengthening information security, strengthening global cooperation against cybercrime. Also, the General Data Protection Regulation (GDPR) of the European Union, as an international standard, is aimed at ensuring the confidentiality and security of personal data. At the national level, a number of laws of the Republic of Uzbekistan, including the Law "On Informatization" and the Law "On Electronic Government", determine the legal framework for ensuring information security.

Keywords: Cybersecurity, international law, Budapest Convention, GDPR, Uzbek legislation, information security, e-government, information technologies.

INTODUCTION

Cybersecurity has become one of the most pressing issues at the international and national levels in the context of the rapid development of modern information technologies. Cybercrimes and illegal misappropriation of information through information technologies pose new challenges for states. Therefore, the international community and national states are paying special attention to strengthening the legal framework to ensure cybersecurity. At the international level, the Budapest Convention and the General Data Protection Regulation (GDPR) of the European Union are the main regulatory documents regulating information security. These documents play an important role in strengthening the fight against cybercrime and protecting personal data on a global scale.

In the Republic of Uzbekistan, the laws "Axborotlashtirish to‘g‘risida", "Elektron hukumat to‘g‘risida" and "Elektron hujjat aylanishi to‘g‘risida" serve as the main legal mechanisms for ensuring cybersecurity. This study systematically analyzes international and national legal norms and broadly highlights their role and importance in strengthening cybersecurity.

LITERATURE REVIEW AND METHODS

International and national legal frameworks on cybersecurity complement each other. At the international level, the Budapest Convention regulates international cooperation against unlawful acts committed through information technologies. The GDPR also establishes strict rules aimed at protecting personal data. At the national level, the Laws of the Republic of Uzbekistan "Axborotlashtirish to‘g‘risida" and "Elektron hujjat aylanishi to‘g‘risida" play an important role in ensuring the security of information systems and digitizing public services. These legal documents are aimed at increasing the efficiency of public systems and protecting personal data.

The study used legal analysis and comparative methods to study international and national regulatory documents. The compatibility of national legislation with international standards was analyzed and practical results were assessed. The interaction of international and national legal frameworks was analyzed through a systematic approach. The legislation of the Republic of Uzbekistan in the field of cybersecurity was compared with international standards, and the level of compatibility between national and international legal standards was analyzed

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

DICUSSION AND RESULTS

The legal foundations of cybersecurity hold strategic importance not only for the international community but also for individual nations. They serve as a critical tool in combating cybercrime and ensuring information security. Among the international legal mechanisms in this field, the Budapest Convention stands out as a pivotal document. Adopted in 2001, this treaty, officially known as the Council of Europe Convention on Cybercrime, establishes a comprehensive legal framework for identifying, investigating, and effectively addressing cybercrimes.

The Budapest Convention primarily focuses on regulating illegal activities conducted through information technologies. It provides detailed provisions for combating crimes such as data breaches, unauthorized system access, and internet-based fraud, while emphasizing the need for international cooperation. This convention serves as a cornerstone for implementing global cybersecurity standards. To date, more than 60 countries have joined the treaty, fostering a new era of collaboration in strengthening digital security and combating cybercrime.

In the system of international legal norms, the General Data Protection Regulation (GDPR) of the European Union, which came into force in 2016, holds particular significance. GDPR introduces strict rules for the protection of personal data and is recognized as a global standard in this field. These regulations are mandatory not only within the European Union but also for companies operating in its jurisdiction. This legal document ensures strong protection of personal data confidentiality and prevents its unlawful use, serving as a relevant example for developing countries like Uzbekistan.

At the national level, Uzbekistan has adopted several important legislative acts to strengthen cybersecurity. The "Law on Electronic Document Circulation," which came into effect in 2004, provides a legal framework for electronic document exchange between government bodies and business entities. This law clearly defines the legal status, authentication, and security of electronic documents, playing a key role in increasing transparency, expediting document circulation, and enhancing system efficiency in the process of digitalizing public services. Another critical piece of legislation is the "Law on Information Security," adopted in 2003, which serves as a key legal foundation for ensuring the stability of information systems in Uzbekistan. This law guarantees the fundamental principles of information security—confidentiality, integrity, and availability. According to its provisions, government bodies, business entities, and citizens must actively participate in ensuring information security and comply with established regulations. It prioritizes identifying cyber threats, developing effective countermeasures, and ensuring security as one of the government's key policy areas.

In implementing national legislation, the UZCERT—Uzbekistan’s National Information Security Center—plays a crucial role. This organization not only focuses on protecting information systems but also organizes activities aimed at training cybersecurity specialists, introducing new solutions in the field, and raising public awareness.

Furthermore, Uzbekistan actively participates in international forums and events, leveraging global expertise and integrating it into its systems to enhance its capacity in cybersecurity. The interconnectedness of international and national legal frameworks creates a solid foundation for developing effective measures against modern cyber threats and ensuring information security. International legal standards like the Budapest Convention and GDPR, alongside Uzbekistan’s national laws such as the "Law on Information Security" and other legislative acts, are critical in ensuring the stable and secure development of information technologies. Collaboration at both national and international levels continues to evolve as a vital strategic approach to combating cybercrime.

Several regulatory and legal documents play a crucial role in regulating activities in cyberspace, including on social media. Among them, the following can be highlighted:

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

- "The Civil Code of the Republic of Uzbekistan": Serves as the primary legal source for protecting information rights and resolving disputes in the field of cyber activities.
- "The Law "On Informatization": Regulates the role and development of information systems and technologies in state policy.
- "The Law "On Electronic Government": Provides the normative framework for regulating digitalization of public services and enhancing their efficiency.
- "The Law "On Electronic Document Circulation": Covers the legal status, security, and identification of electronic documents.
- "The Law "On Payments and Payment Systems": Serves as a fundamental document ensuring the security of payment systems in the digital economy.
- "Resolutions of the Cabinet of Ministers of the Republic of Uzbekistan": Regulatory acts aimed at establishing licensing and permitting procedures through specialized electronic systems.

According to the provisions outlined in Chapter 8 of the General Part of the "Civil Code of the Republic of Uzbekistan", information is classified as an intangible benefit and is considered an object of cyber law. Based on this principle, information constituting official or commercial secrets is subject to protection. If such information is unknown to third parties, possesses actual or potential commercial value, is not legally accessible to others, and its owner takes measures to ensure its confidentiality, it is legally protected.

These norms underline the importance of safeguarding information in cyberspace and provide a robust legal foundation for regulating activities in the digital environment.

The Law of the Republic of Uzbekistan "On Informatization" (adopted on December 11, 2003, No. 560-II) is aimed at regulating relations in the field of informatization. This law establishes key provisions regarding the ownership of information resources and systems, as well as the use of information technologies and systems.

The Law of the Republic of Uzbekistan "On Electronic Document Circulation" (adopted on April 29, 2004, No. 611-II) is one of the significant legal documents developed and adopted to modernize the state document circulation system. Primarily, this law focuses on organizing the procedure for sending and receiving documents through electronic systems. It encompasses rules and regulations related to electronic document circulation, including ensuring the security, legality, and validation of documents exchanged via information systems.

The law serves as a foundational normative and technical framework to ensure the efficient functioning of information systems while addressing technical and legal challenges. By establishing a secure and effective electronic document circulation process, the law facilitates the advancement of digital transformation in document management systems.

The Decree of the President of the Republic of Uzbekistan No. PQ-3245, dated August 29, 2017, aims to enhance state policy for the implementation and development of information and communication technologies (ICT). This decree focuses on improving the efficiency of information systems and transforming them into modern, integrated systems by modernizing project management processes in the ICT sector. It also emphasizes strengthening cooperation among state bodies, the private sector, and other organizations, while defining the role of a unified integrator in the development and maintenance of information systems.

Although there is no single international document governing cyber law comprehensively, international legal instruments and regulations emphasize information security. These documents, particularly those issued by the United Nations (UN), play a crucial role in promoting international

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

cooperation and ensuring security in the use of information technologies. Key UN resolutions related to cybersecurity include:

- **"Developments in the Field of Information and Telecommunications in the Context of International Security" (January 4, 1999)**: This resolution addresses the fundamental aspects of global security in the context of advancements in information technologies.
- **"Developments in the Field of Information and Telecommunications in the Context of International Security" (December 23, 1999)**: This resolution aims to strengthen cybersecurity and ensure secure global information exchange.
- **"Report on Developments in the Field of Information and Telecommunications in the Context of International Security" (November 7, 2002)**: Adopted by the First Committee, it focuses on developing global strategies for managing information security and monitoring the evolution of information technologies.
- **"The Right to Privacy in the Digital Age" (December 16, 2013)**: This resolution emphasizes the need to introduce new legal approaches to ensure the security of personal data in the digital environment.
- **"Outcome Document of the High-Level Meeting of the General Assembly on the Overall Review of the Implementation of the Outcomes of the World Summit on the Information Society" (December 16, 2015)**: This resolution highlights the development of the information society, its security, and the reinforcement of international cooperation.

These international initiatives underscore the importance of safeguarding personal and organizational information while promoting global collaboration to address emerging cybersecurity challenges.

CONCLUSION

The legal foundations of cybersecurity today hold strategic importance not only for the international community but also for national states. International and national legal norms play a crucial role in effectively combating modern cyber threats and ensuring information security. In particular, international documents such as the Budapest Convention and the General Data Protection Regulation (GDPR) serve as the main foundation for preventing cybercrime and strengthening digital security. These documents establish essential approaches for ensuring global security in the field of information technologies and enhancing cybersecurity.

Uzbekistan's cybersecurity legislation is also of great significance in this regard. The Law on Information Security, the Law on Electronic Document Circulation, and other normative documents create a strong foundation for ensuring the security of information systems and digitalizing government services at the national level. Additionally, organizations like UZCERT are actively involved in training cybersecurity professionals and implementing measures to ensure security. Overall, international and national legal mechanisms, working together, provide effective approaches to ensuring information security and combating cybercrime. This collaboration and the regulatory framework serve as a solid foundation for the development of cybersecurity, marking a new phase in the fight against cybercrime.

REFERENCES

1. Fundamentals of Information Security: A Textbook / I. M. Karimov, N. A. Turgunov. Tashkent: Academy of the Ministry of Internal Affairs of the Republic of Uzbekistan, 2016.
2. Council of Europe, "Convention on Cybercrime," 2001.
3. European Union, "General Data Protection Regulation," 2016.

Volume: 4 Issue: 1 | Jan–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

4. Uzbekistan Cybersecurity Center Report (2021). Cybersecurity Status and Strategies. Tashkent.
5. Supreme Assembly of the Republic of Uzbekistan, "Law on Information Security," 2003.
6. Supreme Assembly of the Republic of Uzbekistan, "Law on Electronic Document Circulation," 2004.
7. Constitution of the Republic of Uzbekistan.
8. UZCERT, "Report on International Cooperation," 2021.
9. Appazov, A. (2014). Legal aspects of cybersecurity. University of Copenhagen, 38-42.
10. Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). CYBERSECURITY AS A COMPONENT OF THE NATIONAL SECURITY OF THE STATE. Journal of Security & Sustainability Issues, 9(3).
11. Shopina, I., Khomiakov, D., Khrystynchenko, N., Zhukov, S., & Shpenov, D. (2020). CYBERSECURITY: LEGAL AND ORGANIZATIONAL SUPPORT IN LEADING COUNTRIES, NATO AND EU STANDARDS. Journal of Security & Sustainability Issues, 9(3).
12. Verhelst, A. (2020). Filling global governance gaps in cybersecurity: International and european legal perspectives. International Organisations Research Journal, 15(2), 105-124.
13. Ogu, E. C., Ogu, C., & Oluoha, O. U. (2020). 'Global cybersecurity legislation?'-factors, perspective and implications. International Journal of Business Continuity and Risk Management, 10(1), 80-93.
14. Kosseff, J. (2018, May). Developing collaborative and cohesive cybersecurity legal principles. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 283-298). IEEE.
15. Hiller, J. S., & Russell, R. S. (2013). The challenge and imperative of private sector cybersecurity: An international comparison. Computer Law & Security Review, 29(3), 236-245.