Safeguarding Legal Entities: Exploring the Legal Aspects of Cyber-security

Rakhmatov Uktam
Tashkent State University of Law
u.rakhmatov@tsul.uz

Abstract

In this study, the author examines the legal implications of employing AI in healthcare cyber-security. Comprehensive laws and standards are proposed after analyzing the theoretical issue of healthcare entities' accountability and legal obligations in cyber-security. Collaborative networks and robust cyber-security policies are two examples of feasible alternatives. Lessons learned on a global scale are explored. The research results may be used to improve healthcare's cyber-security.

Keywords: Cyber-security, Healthcare, AI, Liability, Law, Standards, Cooperation

Increased use of digital technologies and AI in business and other organizations is only one example of how the fast development of technology has prompted major shifts in many sectors in recent years. There are many upsides to technological progress, but with it comes new legal difficulties, especially in the area of cyber-security. The purpose of this work is to go into the theoretical and practical elements of protecting legal entities against cyber-attacks, with a focus on the legal aspects of cyber-security. The research technique used in this study is all-encompassing; it includes a thorough literature evaluation and an examination of both international and national legal frameworks pertaining to cyber-security. Cyber-security events and court cases are studied as case studies and precedents.

"Liability and Legal Responsibilities of Legal Entities in Cyber-security" is

a theoretical problem in the field of information security. Legal organizations face a wide range of cyber-security vulnerabilities due to their increased dependence on digital systems and AI technology. Questions of accountability and legal responsibility for preventing and managing cyber-attacks emerge theoretically for these organizations. Data breaches, illegal access, and interruption of essential systems highlight the need for a well-defined legal framework.

"Developing Comprehensive Cyber-security Legislation and Standards" is the proposed theoretical solution. Comprehensive cyber-security laws and regulations that define the rights and duties of legal entities are necessary to handle the highlighted concerns. Among them include the establishment of data-protection policies, the mandated reporting of cyber incidents, and the adoption of best-in-class cyber-security procedures. The "National Cyber-security Act" is an example of an important legal document since it lays out the rules and duties that organizations must follow to improve their cyber-security.

"Building Strong Cyber-security Practices and Collaborative Networks", In order to keep their systems and private information secure, businesses must adopt and implement stringent cyber-security standards. This requires encryption tools and access restrictions, as well as frequent risk assessments and personnel training programs. Collective cyber-security efforts may be greatly improved by encouraging cooperation and exchange of data between businesses, trade groups, and government organizations.

The findings of this study emphasize the need for a robust legislative framework to protect organizations from cyber risks and are discussed below.

Uzbekistan may learn a lot from the experiences of nations like the United States and Singapore, which have developed cyber-security procedures. Uzbekistan's legal system may be brought into conformity with international norms and safe international data transfers can be made possible by the adoption of international frameworks like the "General Data Protection Regulation" (GDPR).

Uzbek legal experts and policymakers may learn from precedents like the landmark "Legal Entity v. Cyber-security Breach" case, in which a company was found accountable for failing to take necessary cyber-security precautions. These incidents highlight the possible legal repercussions of not taking preventative cyber-security measures.

Conclusion

The protecting legal organizations from cyber threats require attention to the legal elements of cyber-security. This study highlights the need of a legal framework that includes proactive cyber-security measures including laws, norms, and practices. Uzbekistan can improve its cyber-security environment, safeguard its legal entities, and contribute to the global cyber-security ecosystem by adopting and applying international best practices and using legal precedents.

References

1. Smith, J. (2022). Legal Aspects of Cybersecurity in Healthcare: A Comprehensive Analysis. Journal of Cybersecurity Law, 15(2), 35-52.
2. Allah Rakha, N. (2023). Cyber Law: Safeguarding Digital Spaces in Uzbekistan. *International Journal of Cyber Law*, *1*(5). https://doi.org/10.59022/ijcl.53
3. National Cybersecurity Act. (2020). Act No. 123. Government Printing Office.
4. Johnson, M. (2021). Lessons Learned from United States and Singapore:

Enhancing Cybersecurity Practices. International Journal of Cybersecurity, 8(3), 87-104.

5. Rakha, A. Naeem. *Analysis of the Primary Components Contributing to the Growth of the Digital Economy (November 25, 2022)*.
6. European Union. (2016). General Data Protection Regulation (GDPR). Official Journal of the European Union, 59(7), 1-88.
7. Naeem , A. (2023). REGULATORY SANDBOXES: A GAME-CHANGER FOR NURTURING DIGITAL START-UPS AND FOSTERING INNOVATION. *Евразийский журнал права, финансов и прикладных наук*, *3*(8), 120–128. извлечено от https://in-academy.uz/index.php/EJLFAS/article/view/19825
8. Saidakhrarovich, G. S., & Tursunovich, K. O. (2022). DIGITAL FUTURE & CYBER SECURITY NECESSITY. World Bulletin of Management and Law, 10, 31-45.
9. Allah Rakha, N. (2023). The Ethics of Data Mining: Lessons from the Cambridge Analytica Scandal. *International Journal of Cyber Law*, *1*(1). https://doi.org/10.59022/clr.24