THE USA JOURNALS
THE AMERICAN JOURNAL OF POLITICAL SCIENCE LAW AND CRIMINOLOGY (ISSN- 2693-0803)
VOLUME 06 ISSUE01

PUBLISHED DATE: - 31-01-2024
DOI: - https://doi.org/10.37547/tajpslc/Volume06Issue01-19 **PAGE NO.: - 97-99**

RESEARCH ARTICLE **Open Access**

LEGAL ISSUES OF DIGITIZATION IN ENVIRONMENTAL LAW

Durbek MAKHKAMOV
DSC, Associate Professor, Tashkent State University Of Law, Uzbekistan

Abstract
Environmental law is a very broad field. Therefore, we study it as a complex legal system. Today, the dynamics of digitization processes also affect environmental law. This article is devoted to the issue of legal regulation of problems arising in these relations. No research has been conducted on cyber security issues in environmental legislation in Uzbekistan. The article contains a number of analyzes and suggestions. In our opinion, this article is the first stage of research on this topic.

Keywords Cybersecurity in environmental law, natural resources, digitalization, legal regime, Internet of Things in environmental law.

INTRODUCTION

Although several studies have investigated the role of digitalization in various economic, social, and environmental factors, most of these studies have provided empirical evidence regarding the developmental, social, and environmental impact of digitalization. Still, these studies are limited in several ways. For instance, the existing studies merely mentioned the detailed or influential channels (a mechanism) through which digitalization affects sustainable development, social development, and environmental quality. Besides, these studies are limited to the investigation of a particular country or region while lacking the generalizability or general overview regarding the influence of digitalization on these three sectors. Following such limitations in the existing literature, this research tends to provide a generalized overview, adoption, implementation, and effective mechanism through which digitalization could be favorable for sustainable development, social development, and environmental sustainability. Since the earlier studies focus on the influence of digitalization in a specific region and a specific sector, i.e., either economic, financial, or environmental. Unlike the existing strand of literature, this study provides a thorough overview of the influence on cybersecurity in environmental law.

METHODS

In the preparation of this scientific article, logical and scientific methods of scientific knowledge were used, in particular, logical analysis, historical, comparative legal methods were used.

RESULT

As technology continues to advance and the world becomes increasingly digital, we are generating and sharing more data than ever before. At the same time, we are facing unprecedented environmental challenges that require innovative solutions. To address these challenges, we need to ensure that sensitive environmental data is protected from cyber threats and that our cyber defenses are in compliance with environmental regulations.

With that in mind, let's focus on five key issues related to the role of cybersecurity in

environmental law.

1. Data Breaches: The first issue is data breaches. Environmental data is valuable and can be used by hackers for malicious purposes. For example, data about protected species or natural resources could be used for illegal extraction or trafficking. To prevent this, environmental law needs to incorporate cybersecurity measures to protect sensitive data. One example of a legal solution is the European Union's General Data Protection Regulation (GDPR) (Jorgensen and Leister, 2018), which requires companies to take steps to protect personal data from cyber threats.

2. Cloud Computing: The second issue is cloud computing. Many organizations, including those involved in environmental protection, store data in the cloud. However, the cloud is not immune to cyber threats, and the risks associated with storing sensitive data in the cloud need to be addressed by environmental law. An example of a legal solution is the United States Federal Risk and Authorization Management Program (FedRAMP) (NIST, 2013), which provides a standardized approach to security assessment and authorization for cloud services.

3. Internet of Things (IoT): The third issue is the Internet of Things (IoT). IoT devices are increasingly being used to monitor environmental conditions, such as air and water quality. However, these devices are also vulnerable to cyber threats, and environmental law needs to ensure that the use of IoT devices is in compliance with cybersecurity regulations. An example of a legal solution is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2018), which provides guidelines for securing IoT devices.

4. Cross-Border Data Transfers: The fourth issue is cross-border data transfers. Environmental data is often shared across borders for scientific research and policy-making purposes. However, different countries have different data protection laws, and the transfer of sensitive environmental data needs to be done in compliance with these laws. An example of a legal solution is the European Union's General Data Protection Regulation (GDPR) (Jorgensen and Leister, 2018), which regulates the transfer of personal data outside the EU.

5. Cybersecurity Capacity Building: The fifth issue is cybersecurity capacity building. Many organizations involved in environmental protection may not have the expertise or resources to implement effective cybersecurity measures. Environmental law needs to promote capacity building to ensure that all organizations have the ability to protect sensitive environmental data. An example of a legal solution is the African Union Convention on Cybersecurity and Personal Data Protection (AUC, 2014), which includes provisions for capacity building and technology transfer.

Analysis of research results

Here are some recommendations for legislation in Uzbekistan regarding the role of cybersecurity in environmental law:

1. Develop specific legislation that focuses on cybersecurity in environmental law. This would help to ensure that environmental data is protected from cyber threats and that cybersecurity measures are in compliance with environmental regulations.

2. Establish a regulatory framework that mandates cybersecurity compliance for all organizations involved in environmental protection. This could include regular audits and assessments to ensure that cybersecurity measures are in place and up to date.

3. Promote capacity building and training for organizations involved in environmental protection to ensure that they have the expertise and resources to implement effective cybersecurity measures.

4. Encourage the adoption of international legal solutions, such as the European Union's General Data Protection Regulation (GDPR) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, to ensure that cybersecurity measures are consistent with global standards.

5. Facilitate cross-border data transfers of environmental data by developing legal frameworks that ensure that sensitive

environmental data is protected during transit and complies with data protection laws in different jurisdictions.

CONCLUSION

By implementing these recommendations, Uzbekistan can ensure that cybersecurity measures are in place to protect sensitive environmental data and that organizations involved in environmental protection are in compliance with relevant cybersecurity regulations.

In conclusion, the role of cybersecurity in environmental law is crucial in ensuring the protection of sensitive data in the age of digitization. By addressing the five key issues I have outlined, environmental law can promote sustainable development and protect the planet for future generations.

REFERENCES

1. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9748610/#:~:text=Digitalization%20enhances%20technological%20innovation%2C%20which,emissions%20and%20other%20pollution%20levels.
2. Jorgensen, R. and Leister, R., 2018. EU General Data Protection Regulation (GDPR). The Privacy Advisor. [Online] Available at: https://iapp.org/news/a/eu-general-data-protection-regulation-gdpr/ [Accessed 10 July 2021].
3. NIST, 2013. Federal Risk and Authorization Management Program (FedRAMP). NIST Special Publication 800-37. [Online] Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf [Accessed 10 July 2021].
4. NIST, 2018. Internet of Things (IoT). National Institute of Standards and Technology. [Online] Available at: https://www.nist.gov/programs-projects/internet-things-iot [Accessed 10 July 2021].
5. Jorgensen, R. and Leister, R., 2018. EU General Data Protection Regulation (GDPR). The Privacy Advisor. [Online] Available at: https://iapp.org/news/a/eu-general-data-protection-regulation-gdpr/ [Accessed 10 July 2021].
6. African Union Commission (AUC), 2014. Convention on Cybersecurity and Personal Data Protection. African Union. [Online] Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection [Accessed 10 July 2021].