LEGAL BASES OF INFORMATION SECURITY IN ELECTRONIC COMMERCE

Nazarova G
TUIT, Teacher

ANNOTATION:

This article discusses the legal basis for ensuring information security in e-commerce. The authors analyze national and international laws governing data protection, privacy and cybersecurity in the context of online transactions.

Keywords: Information security, e-commerce, data protection, privacy, cybersecurity.

INTRODUCTION:

E-commerce is developing rapidly, which leads to a growing need to protect confidential information and prevent cybercrime. Legal frameworks play a crucial role in ensuring the security of electronic transactions and protecting the rights of both consumers and businesses.

National laws:

• Personal Data Protection Act (GDPR): The European Union has established strict personal data protection rules applicable to all companies processing data of EU data subjects.

• Information Protection Act (PIPEDA): Canada has passed a comprehensive law protecting personal information in commercial transactions.

• California Consumer Privacy Protection Act (CCPA): California has developed its own law giving consumers more rights to control their personal information.

International agreements:

• Council of Europe Convention on Cybercrime (Budapest Convention): The first international treaty criminalizing cybercrime, including unauthorized access, data interception and fraud.

• The Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Cross-border Flows of Personal Data:

Provide guidance to countries on developing data protection laws and ensuring the free cross-border flow of data.

Cybersecurity:

• Cybersecurity Improvement Act (CISA): The United States has passed legislation aimed at improving the exchange of information about cyber threats and coordinating responses to cybersecurity.

• The European Union Directive on the Security of Networks and Information Systems (NIS): Requires organizations in vital sectors such as energy and healthcare to take measures to manage cybersecurity risks.

In the era of digital transformation, e-commerce has become an integral part of the modern economy. It provides convenience, accessibility and a wide range of goods and services to consumers around the world. However, the growth of e-commerce has also led to new risks and threats to information security.

Protecting confidential information, preventing cybercrime, and ensuring the integrity and accessibility of online systems are crucial to maintaining consumer and business confidence in e-commerce. The legal framework plays a central role in setting the framework for information security in this rapidly developing field.

In this article, we will consider the legal basis for ensuring information security in e-commerce. We will analyze national and international laws governing data protection, privacy and cybersecurity in the context of online transactions. An understanding of this legal framework is necessary for all stakeholders in e-commerce, including businesses, consumers and regulators, to ensure a safe and reliable online environment.

• UN General Assembly Resolution A/RES/74/247 on the right to privacy in the digital age: Reaffirms the right to privacy as a fundamental human right and calls on States to take measures to protect it in the context of the rapid development of digital technologies.

• The International Telecommunication Union (ITU) Guidelines on Cybersecurity: Provide guidance to countries on the development and implementation of comprehensive cybersecurity strategies, including measures to protect critical infrastructure and ensure resilience to cyber attacks.

• The World Economic Forum Report on Global Risks 2023: Identifies cybersecurity as one of the main global risks, emphasizing the need for international cooperation and innovative approaches to managing cyber threats.

• The European Cybersecurity Agency (ENISA) study on cybersecurity risks for small and medium-sized enterprises: Identifies common cybersecurity vulnerabilities and risks faced by small and medium-sized enterprises and offers practical recommendations on how to mitigate them.

• The Alliance for an Accessible Internet (A4AI) Cybersecurity Law Database: Provides a comparative overview of cybersecurity laws in various countries around the world, facilitating analysis and sharing of best practices.

These additional materials expand the understanding of the legal foundations of information security in e-commerce by providing an international perspective, industry recommendations and practical guides for organizations of all sizes.

DISCUSSION:

The legal framework for information security in e-commerce provides a framework for data protection, privacy, and cybersecurity. These laws and agreements set minimum standards for the processing and transfer of personal information, criminalize cybercrime, and require organizations to take measures to protect their systems from cyber threats.

CONCLUSION:

Legal frameworks play an important role in providing a safe and secure environment for e-commerce. Constantly evolving technologies and growing cyber threats require regular updating and adaptation of the legal framework. Cooperation between governments, businesses and law enforcement agencies is crucial to protect information security in e-commerce and ensure consumer confidence in online transactions.

REFERENCES

1.See Official Records of the Economic and Social Council, 2013, Supplement No. 10 and corrigendum (E/2013/30 and E/2013/30/Corr.1), chap. I, sect. D.

2. Resolution 70/174, annex.

3. A/65/201, A/68/98 and A/70/174.

4. See Official Records of the Economic and Social Council, 2017, Supplement No. 10 (E/2017/30), chap. I, sect. D.