Volume 1 Issue 2 (2024) 27-32
E-ISSN 2988-6740 | © Authors. CC BY-SA
https://doi.org/10.59261/iclr.v1i2.4
https://iclr.polteksci.ac.id/

Indonesian Cyber Law Review

The Role of Cyber Law in Maintaining Digital Economic Security in Indonesia: a Study of E-Commerce and Online Transaction Security

Diana Magfiroh[1], Elvira Fitrianti[2], Pegi Sugiartini[3]
[1] Universitas Cendekia Mitra Indonesia, Yogyakarta, Indonesia
[2] Politeknik Siber Cerdika Internasional, Cirebon, Indonesia
[3] Universitas Muhammadiyah Cirebon, Indonesia
Corresponding email: dianamagfiroh0002@gmail.com

ABSTRACT

Indonesia's digital economy is growing rapidly with e-commerce transactions continuing to increase. However, this is accompanied by increasing cyber threats that endanger the security of online transactions. Cyber law, through the ITE Law and the Personal Data Protection Law, plays a vital role in maintaining the security of these transactions, but its implementation still faces various challenges. This study aims to analyze the effectiveness of cyber law in protecting the security of e-commerce transactions in Indonesia, identify gaps in regulations, and provide recommendations for improving digital security. This study uses a qualitative method with a descriptive-analytical approach. Data were collected through in-depth interviews with experts and document analysis related to cyber law regulations and security incident reports. Samples were selected purposively from regulators, cybersecurity experts, and e-commerce representatives. The results of the study show that although cyber law regulations already exist, their implementation is not optimal. Many business actors have not complied with security standards, and law enforcement against violations is still weak. In addition, the National Cyber and Crypto Agency (BSSN) has an important role, but limited resources and coordination are obstacles. Public education about cyber security also still needs to be improved. Stronger collaboration between the government, private sector, and the community is needed to improve the security of online transactions, as well as stricter enforcement of regulations to create a safer e-commerce ecosystem in Indonesia. Cyber law, transaction security, e-commerce, data protection, regulation

Keywords: *Cyber law, transaction security, e-commerce, data protection, regulation*

1. Introduction

The development of the digital economy in Indonesia is increasingly rapid, especially with the rise of e-commerce platforms used by the public (Jannah et al., 2025; Lestari et al., 2024). Data from the Central Statistics Agency (BPS) shows that the number of e-commerce transactions in Indonesia has increased significantly in recent years, reaching a value of IDR 108.54 trillion in 2021. Although this growth has

contributed greatly to the national economy, there are significant challenges related to the security of online transactions. The inclusion of the role of cyber law is very crucial to maintaining the security of the digital economy in Indonesia.

Security in online transactions is a major concern for governments and businesses. Based on a report from Kaspersky, Indonesia ranks highest in the number of cyber attacks in Southeast Asia in 2022, with the e-commerce sector as one of the main targets. Therefore, in-depth research is needed on the role of cyber law in addressing this threat and how existing legal policies are able to provide sufficient protection.

Based on data from BSSN (National Cyber and Crypto Agency), it can be seen that the number of cyber incidents increased from 189 million in 2020 to 290 million in 2022 (Partipilo & Stroppa, 2023). Several previous studies have discussed the issue of digital security in Indonesia, but few have focused on the cyber law aspect of e-commerce. For example, a study by Hapsari discusses cyber threats to online businesses, but has not examined the applicable legal policies in detail. Meanwhile, study explores cyber law challenges, but has not discussed them specifically with e-commerce transaction security.

Based on previous research, there is a specific research space between the role of cyber law and online transaction security in the context of e-commerce in Indonesia (Rahman et al., 2024; Santoso, 2022). Most studies focus more on the technical aspects of cyber security without a comprehensive examination of the effectiveness of existing legal regulations.

This study offers novelty by exploring the direct relationship between cyber law and e-commerce transaction security in Indonesia. The main focus of this study is on how current regulations are able or not to ward off cyber threats, as well as providing analysis of policies that need to be improved.

The purpose of this study is to analyze the effectiveness of cyber law in maintaining the security of online transactions in the e-commerce sector in Indonesia. This study is expected to provide recommendations for the government and regulators regarding policy improvements in order to protect the digital economy from cyber threats.

2. Method

This study uses a qualitative research method with a descriptive-analytical approach. This approach was chosen because this study aims to understand the phenomena related to the role of cyber law in maintaining the security of e-commerce transactions in Indonesia, through existing analysis and case studies related to cyber-attacks in online transactions. Qualitative research provides an overview in digging up in-depth information from various related sources, such as laws, policies, and security incident reports. The population of this study includes all institutions and individuals related to cyber regulation and security in Indonesia, including regulators such as the Ministry of Communication and Informatics (KOMINFO), the National Cyber and Crypto Agency (BSSN), and e-commerce players in Indonesia. The research sample was selected purposively, where the main sample that is the focus of this study

is legal officials involved in the preparation of cyber policies, cybersecurity experts, and representatives from leading e-commerce companies in Indonesia. Purposive sample selection was carried out to obtain relevant information from sources who have knowledge and direct involvement in the issues being studied. Document analysis was used to review regulations, laws, and reports related to cybersecurity and e-commerce in Indonesia, such as the ITE Law (Information and Electronic Transactions) and the annual report from BSSN regarding cyber incidents. The data was analyzed using thematic analysis techniques, where data obtained from interviews and documents will be coded based on certain themes relevant to the role of cyber law in maintaining the security of e-commerce transactions.

3. Result & Discussion

Effectiveness of Cyber Law in Protecting E-commerce in Indonesia

The results of the study show that the implementation of cyber law in Indonesia, especially related to e-commerce transactions, is still not optimal (Rahman et al., 2024; Santoso, 2022). Although the ITE Law (Electronic Information and Transactions Law) has been passed since 2008, several important aspects, such as consumer data protection and law enforcement against cybercriminals, have not been fully implemented. This can be seen from the many cases of fraud and personal data violations that have befallen e- commerce consumers.

One of the main problems is the gap between existing regulations and their implementation in the field. Many e-commerce business actors have not fully complied with regulations related to transaction security and data protection, especially small and medium enterprises (SMEs) that lack the resources to comply with cybersecurity standards set by the government. In addition, cyber law in Indonesia also still faces challenges in terms of harmonization with international regulations required for cross-border transactions.

Another obstacle identified in this study is the lack of legal awareness among the public and e-commerce business actors (Volynets et al., 2024). Although there are clear regulations, many internet users still do not understand their rights and obligations in the context of online transactions. Cyber law education needs to be improved so that the public is more aware of possible threats in the digital world.

The Role of the National Cyber and Crypto Agency (BSSN) in Online Transaction Security

BSSN plays an important role in monitoring and handling cybersecurity incidents in Indonesia, including in the e-commerce sector (Bhakti et al., 2024; Marwan et al., 2022). From the analysis of BSSN documents, it is clear that cyber law enforcement efforts are often hampered by coordination agreements between the parties involved, including between BSSN and law enforcement officers, such as the police and prosecutors. For example, when a personal data breach occurs, the investigation process often takes a long time, which ultimately harms e-commerce consumers. In addition, BSSN also faces challenges in terms of developing dynamic regulations to adapt to rapid technological developments.

In facing these challenges, BSSN has proposed several solutions, including closer cooperation with technology companies and e-commerce platform providers in terms of sharing cyber threat data and joint mitigation efforts (Belghith, 2024; Brustinov, 2024). However, the implementation of these initiatives still requires strict supervision to be effective in dealing with threats.

Regulatory Gaps and Consumer Data Protection

This study found a gap in regulations related to consumer data protection in online transactions (Zhang et al., 2020). Although the Personal Data Protection Law (UU PDP) was passed in 2022, its implementation is still not optimal. Many e-commerce platforms, especially smaller ones, have not adopted adequate security systems to protect consumers' personal data.

These regulations are also not fully integrated with business practices in the field. For example, in the case of a data leak involving a large e-commerce platform, law enforcement is still weak, with minimal fines or sanctions given to negligent companies. This shows that despite progress in policy formulation, gaps in implementation and enforcement remain a challenge (Ménard et al., 2020). Consumers also face challenges in understanding their rights when it comes to data security. Most consumers are unaware that they can complain if their personal data is misused in online transactions. The study recommends increasing educational campaigns that focus on consumer rights in the digital age, including personal data protection and steps that can be taken in the event of a breach.

Efforts to Improve Cyber Security in Indonesia

To improve cybersecurity in the e-commerce sector, more strategic steps are needed(Atkins & Lawson, 2021; Gupta, 2024; Liu et al., 2022). One of the main recommendations that emerged from this study is the need for stricter law enforcement against cybercriminals, especially in the context of online transactions. The government must be more proactive in developing regulations that are adaptive to technological developments, as well as strengthening sanctions for companies that do not comply with cybersecurity standards.

In addition, there needs to be more intensive collaboration between the private sector and the government in building a stronger cybersecurity infrastructure . For example, e-commerce platform providers can start with the government to share threat data and early detection technology that can accelerate the identification and mitigation of cyber attacks. The implementation of strict cybersecurity standards must also be applied not only to large companies, but also to SMEs engaged in e-commerce.

This study also suggests the importance of educating the public to raise awareness about cybersecurity. Consumers should be encouraged to be more careful in conducting online transactions, such as using secure networks, avoiding storing sensitive data openly, and utilizing more secure authentication methods. All of these efforts will help strengthen the cybersecurity ecosystem in Indonesia, especially in maintaining the security of the digital economy.

4. Conclusion

This study reveals that cyber law in Indonesia, although regulated through the ITE Law and the Personal Data Protection Law (UU PDP), still faces serious challenges in its implementation to maintain the security of e-commerce transactions. One of the main findings is the gap between existing regulations and implementation in the field, especially in terms of law enforcement against cyber violations and consumer data protection. Many business actors, especially SMEs, have not complied with the established security standards, so consumers often become victims of fraud and data breaches. The role of the National Cyber and Crypto Agency (BSSN) is also considered important but still requires improvement in terms of coordination and resource capacity.

In addition, this study highlights the need for further education for the public and business actors regarding cyber law and data protection. Despite efforts, many consumers are still unaware of their rights in online transactions, and many business actors do not pay attention to the importance of cybersecurity. The conclusion of this study is that collaboration between the government, the private sector, and the community is essential to create a safer e-commerce ecosystem. In addition, more dynamic regulations and strict law enforcement need to be implemented to address cybersecurity challenges in the digital era.

5. References

Atkins, S., & Lawson, C. (2021). An improvised patchwork: success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5), 847–861.

Belghith, A. (2024). e-CommerceShield: A Framework for Enhanced Security in E-Commerce with Awareness, DNS Matching, and Blockchain Integration. *2024 IEEE 30th International Conference on Telecommunications (ICT)*, 1–6.

Bhakti, A., Sudirman, A., Sumadinata, R. W. S., & Bainus, A. (2024). State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia. *Journal of Human Security*, *20*(1), 109–117.

Brustinov, V. (2024). *Management of information security of the company (based on Business Media Network case)*. Private Higher Educational Establishment-Institute "Ukrainian-American ….

Gupta, R. (2024). Cybersecurity Threats in E-Commerce: Trends and Mitigation Strategies. *Journal of Advanced Management Studies*, *1*(3), 1–10.

Jannah, M., Mahmuda, Z., & Alankrita, A. (2025). The Digital Economy Boom: How E-Commerce is Reshaping Indonesia's Market. *Indonesia Discourse*, *2*(1).

Lestari, A. P., Fatiha, S. A., & Putri, S. O. (2024). E-Commerce in Indonesia's Economic Transformation and Its Influence on Global Trade. *International Journal of Computer in Law & Political Science*, *4*, 10–23.

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, *13*, 927398.

Marwan, A., Jiow, H. J., & Monteiro, K. (2022). Cybersecurity regulation and

governance during the pandemic time in Indonesia and Singapore. *International Journal of Global Community*, *5*(1), 13–32.

Ménard, C., Jimenez, A., & Tropp, H. (2020). Addressing the policy-implementation gaps in water services: the key role of meso-institutions. *OECD Principles on Water Governance*, 13–33.

Partipilo, F. R., & Stroppa, M. (2023). Humanitarian organisations under cyber-attack: emerging threats and humanitarian actors' responsibilities under international human rights law. In *Responsible Behaviour in Cyberspace: Global Narratives and Practice* (pp. 238–257). Publications Office of the European Union.

Rahman, I., Muhtar, M. H., Mongdong, N. M., Setiawan, R., Setiawan, B., & Siburian, H. K. (2024). Harmonization of Digital laws and Adaptation Strategies in Indonesia focusing on E-Commerce and Digital transactions. *Innovative: Journal Of Social Science Research*, *4*(1), 4314–4327.

Santoso, E. (2022). Opportunities and challenges: e-commerce in Indonesia from a legal perspective. *Jurnal Penelitian Hukum De Jure*, *22*(3), 395–410.

Volynets, V., Lohvynenko, V., Korobka, S., Kuzmenko, O., & Derhaliuk, M. (2024). E-commerce development: Prospects and legal challenges of business digital transformation amidst economic de-shadowing. *Multidisciplinary Reviews*, *8*.

Zhang, J., Hassandoust, F., & Williams, J. E. (2020). Online customer trust in the context of the general data protection regulation (GDPR). *Pacific Asia Journal of the Association for Information Systems*, *12*(1), 4.