



Cybersecurity Regulation in Online Commerce: Data Protection Protection and Security Threats

Falihatun Nabila¹, Siti Marwa², Mochammad Reza Adiyanto³
Management Department, Trunojoyo Madura University

ARTICLE INFO

Abstract

Keywords:

Cyber Security, Online
Commerce, Data Protection,
Standardization system

Cybersecurity is an important foundation for personal data protection, current technological developments continue to lead to the use of data as a very influential and valuable thing. In the economic aspect, trade has also implemented an online system as an effort to attract consumers because it is considered easier and shortens time. However, this is inseparable from the possible risks in implementing the system and ensuring security. The state plays a role in developing regulations on personal data protection and cybersecurity. Data protection and security enhancement requirements have not been included in any regulations, making cases of rampant cyber incidents continue to occur due to the absence of established standards. For this reason, it will look at how the need to meet the data protection requirements and security guarantees included in a regulation so that all online trading sites and applications can have the right systems in place to protect data and minimize security threats. The author chooses a qualitative method to facilitate the collection of data obtained through books, journal articles, online media, or libraries and other sources. The results of the study show that the data protection and security system is not optimal, and cybersecurity regulations must also implement standardization to realize citizens' rights to their data.

✉ Correspondent
(*) Author

Email:
falihatunnabila85@gmail.com¹, sitimarwa1121@gmail.com²,
reza.adiyanto@trunojoyo.ac.id³

E-ISSN: 3026-0965

DOI :

INTRODUCTION

The development of technology has affected every aspect of life, including businesses that have always had every way to promote the trade of both goods and services to be recognized in a wider scope. In this case, the development that has been carried out in realizing the promotional goals is the development of an "Online" trading system or often called "e-commerce" to facilitate access to the remote trading system, minimizing the use of paper as a medium of transactions and a medium of

agreement or coordination. Online purchase refers to the transaction process that occurs between the seller and the buyer on the website (Wantara, Suryato. 2023).

The rapid growth of the "Online" trading system will also affect the potential risks that will arise. Everything managed by the system will have a weak side where it is the state's liability for the incident that has occurred. Currently, the most common case is the rampant leakage of customer or e-commerce user data, which is generally caused by negligent or weak security systems. The incident has a negative impact on consumers, where consumers are targeted to potentially receive product offers, services, or information from sellers. In addition, in making transactions, consumers are required to register, transact, and pay, which requires the input of confidential personal data (Rohmah, 2022). So that potential consumers become victims and as the party who feels the most unlucky and rarely gets satisfactory compensation to overcome data that has been leaked and has been widely spread. In addition, potential consumers are also internet users who use the internet to communicate and make transactions, sell goods, do business, and work (Andriani. et al, 2022).

All risks and incidents that occur are the state's obligation to make regulations to reduce data leakage and improve cybersecurity in the e-commerce system. Factually speaking, the government has tried to form regulations related to cyber security which are regulated in Law Number 11 of 2008 concerning Electronic Information and Transactions Jo. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems (PP PSTE), Law Number 27 of 2022 concerning Personal Data Protection. The regulations that have been formed do not allow the risk of data leakage to not occur again because it only includes sanctions for risks that have occurred with the intention of harming many parties. The era of globalization has always been marked by rapid changes in overall economic conditions which have caused a number of demands to arise in response to the changes that occur (Safrizal. et al, 2020).

Much needs to be improved on regulations to strengthen the security system in e-commerce. In an increasingly advanced era, the improvement of systems and technology from year to year continues to be improved to be more sophisticated, knowing the responsible party is not enough but there needs to be regulations that do regulate the improvement of security systems rather than the implementation of e-commerce electronic systems so that all risks do not occur again. Based on the background discussed, it can be formulated how to regulate data leaks and cybersecurity in online commerce (e-commerce) in Indonesia? and what solutions can be done to improve the cybersecurity of e-commerce online commerce in Indonesia?

LITERATURE REVIEW

1. Cyber Security

Cybersecurity is derived from the United Kingdom words "Cyber" and "Security", which are etymologically defined and commonly known as the scope of cyberspace, the internet, or information technology (IT). Cybersecurity serves to address, detect, find, counteract, or minimize the level of risk to disruptions, cyber threats, and cyberattacks. In addition, it also includes all cyber technology activities that can threaten the security of all components in cyber systems, including hardware, software, data/information, and infrastructure (Siagian et al., 2017).

One form of cybercrime activity involves aspects of negative content, which can be grouped into several categories, namely: 1) violations of the confidentiality, integrity, and availability of data and computer systems; 2) computer-related breaches; 3) content-related violations; and 4) copyright infringement (Siagian et al., 2017).

2. Online Commerce (E-commerce)

In the era of globalization which is marked by the rapid advancement of information technology, the development of entrepreneurial marketing strategies that are able to reach all consumers in various parts of the world is needed, especially through the use of internet marketing or E-Commerce. Easy access to information provided by internet media is increasing, supported by the growth of adequate infrastructure (Moor et al., 2009). Rahmanti (2009) Electronic Commerce or e-commerce can be defined as a marketing system that uses electronic media. E-commerce involves the distribution, sale, purchase, marketing, and service of products through electronic systems, such as the internet or in other forms of computer networks. Internet marketing brings five major advantages to companies that adopt it. First, both large and small companies can apply it. Second, there are no physical limitations in the advertising space compared to print and broadcast media. Third, access and retrieval of information is very fast compared to express mail or even fax. Fourth, the site can be accessed by anyone, anywhere, and anytime. Fifth, the purchasing process can be carried out faster and independently (Kotler in Widodo, 2002). Digitalization gives greater power to customers and makes business people think about how to win the market (Jannah, 2021).

3. Data Protection

The protection of personal data is considered part of efforts to protect human rights. Therefore, regulations related to the right to privacy related to personal data are a form of recognition and protection of human rights. In the context of international relations, Indonesia is expected to meet the demands of data and personal information protection, which can support the smooth running of transnational trade, industry, and investment (Hukum, 2020).

RESEARCH METHODS

The method applied in this study is a qualitative descriptive method. Sugiyono (2016) emphasized that qualitative research methods are used to investigate the natural conditions of objects, where researchers play the role of the main instrument. Nazir (2014) explained that descriptive research focuses on analyzing the status of a group of people, objects, conditions, thought systems, or current events with the aim of producing a systematic, factual, and accurate description of the facts studied. Sukmadinata (2011:73) stated that qualitative descriptive research aims to explain and describe existing phenomena, both natural and man-made, with an emphasis on characteristics, quality, and linkages between activities.

This research is conducted with the aim of gathering up-to-date and detailed information, identifying problems, conducting comparisons or evaluations, and determining the steps taken by others in dealing with similar problems, in the hope of learning from their experiences to plan and make decisions in the future. Thus, qualitative descriptive research only focuses on describing the response to the situation, event, or phenomenon that occurs, without requiring the explanation of causal relationships or hypothesis testing.

The data collection method applied in this study is a literature review, where data sources are obtained from scientific writings such as articles and journals. According to Marzuki (2017), data collection techniques using library research or literature review involve primary legal materials, secondary legal materials, and tertiary legal materials. The applied data analysis approach is a qualitative analysis technique, where all the secondary data collected will be systematically arranged, categorized based on identified themes and patterns, and interpreted to understand the meaning of the data in a social context. The interpretation process is carried out from the researcher's perspective (Diantha, 2017).

RESULTS AND DISCUSSION

Along with the rapid advancement of time and technology, the presence of the internet has become ubiquitous among the global population. The internet facilitates access to anything according to the wants and needs of its users. One of the technological advances or convenience for internet users is access to e-commerce. The buying and selling process, which was previously limited to conventional methods, can now be done electronically through an internet platform. According to Statista Market Insights data, the number of e-commerce users in Indonesia reached 178.94 million people in 2022. This figure represents an increase of 12.79% compared to the previous year which experienced an increase of only 158.65 million users. Looking at current trends, e-commerce users in Indonesia continue to grow, with the number projected to reach 196.47 million users by the end of 2023. This figure is expected to continue to increase in the next four years.

The existence of the buying and selling process in e-commerce is certainly inseparable from online transactions to fulfill the buying and selling process. Bank Indonesia (BI) noted that in 2022, the value of e-commerce transactions in Indonesia reached IDR 476.3 trillion. This data comes from 3.49 billion transactions that occurred on e-commerce platforms during the previous year. Future projections also show a tendency to increase the value of e-commerce transactions in the coming years.

According to the scientific journal "The Utilization of E-commerce in the Business World" by Irmawati (2011), Electronic Commerce, commonly known as E-commerce, is the process of buying and selling or exchanging products and services carried out through internet media. The scope of E-commerce is not limited to business or trade activities but also involves other sectors such as banking services to customers, fintech industry, tourism sector, labor recruitment, and insurance. As an innovation, fintech makes it easier for customers to transact, for example e-money (Purnomo et al, 2021).

The convenience experienced in various sectors is not free from possible risks in the implementation of systems and security guarantees. The state plays an important role in making regulations for personal data protection and cybersecurity. In Indonesia, the government has adopted several regulations related to cybersecurity and personal data protection in the context of e-commerce. This regulation aims to protect consumers, companies, and personal data from potential risks of data leakage and misuse. There are several regulations governing cybersecurity and data protection in Indonesia, including:

- a. Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE). This law serves as a legal framework that covers legal and criminal aspects in the use of information technology, including online commerce or e-commerce. In the context of e-commerce, the ITE Law provides a legal basis

for all actions against cybercrime, including data breaches. On April 29, 2008, this law was enacted as the first cyber law in Indonesia.

- b. Government Regulation of the Republic of Indonesia Number 82 of 2012 concerning Electronic Systems and Electronic Transactions. This regulation provides guidelines on the security of electronic systems and transactions. It covers the cybersecurity aspects that e-commerce service providers need to consider to protect customer data and transactions.
- c. Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. This regulation further regulates the implementation of electronic systems and transactions, including security requirements and personal data protection.
- d. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. This regulation establishes standards for the protection of personal data, including in the context of e-commerce. This entails processing personal data with specific security standards and mandates notification to the relevant authorities in the event of a data breach.
- e. Security Protection Policy. In addition to specific regulations on cybersecurity and personal data, there are also aspects of consumer protection in consumer laws that apply in Indonesia. This protection includes the consumer's right to the privacy and security of users' personal information.

Regulations set by the states or governments mentioned above serve as a legal basis for engaging e-commerce managers in maintaining cybersecurity and data protection. However, laws remain laws, and regulations remain regulations, each with inherent weaknesses in their implementation. For example, in the ITE Law, which became the first cyber law in Indonesia. Despite the comprehensive provisions in the Electronic Information and Transactions Law on cybercrime and data breaches, some articles are considered insufficient in addressing these issues. This can make it difficult for law enforcement in the ever-evolving cybersecurity landscape.

In addition, certain provisions in the Electronic Information and Transactions Act impose seemingly severe penalties, including lengthy prison sentences and hefty fines. This can instill excessive fear and increase the risk of abuse of the law. Although there are regulations related to the protection of personal data, the main focus of the Electronic Information and Transactions Law is on cybercrime in general. This can result in less detailed and less stringent personal data protection regulations. Some of the terms in the law are also ambiguously defined, which leads to diverse interpretations and legal uncertainty, especially when dealing with cybercrime and data breach cases.

Unbeknownst to you, due to the rapid advancement of technology, the Electronic Information and Transaction Law may not immediately accommodate issues that arise in the realm of cybersecurity. This creates legal loopholes or an inability to respond quickly to new threats. It can also be said that the Law on Electronic Information and Transactions is inadequate in providing clear and focused

guidelines or regulations on the obligation of companies to report cybersecurity incidents to the relevant authorities or affected parties.

Laws and regulations are not static entities; They continue to evolve with the advancement of time and technology. This applies to regulations governing cybercrime and data breaches. Despite existing regulations such as the Electronic Information and Transaction Law and the aforementioned ones, the legal landscape in Indonesia cannot turn a blind eye to the realities on the ground that show the dire consequences of rapid technological advancement. This causes irresponsible individuals to become increasingly adept at exploiting existing regulations.

In existing regulations or laws, there is a lack of specificity in detailing good and appropriate security standards, thus minimizing the possibility of data breaches and cybercrimes. However, to prevent data leaks and preserve information, especially in the context of online commerce (e-commerce), there are several regulations and security standards that can be adopted, including:

- a. ISO/IEC 27001: an international standard for information security management. This standard provides a framework for identifying, managing, and mitigating information security risks, including aspects related to e-commerce.
- b. GDPR (General Data Protection Regulation): an EU regulation that provides personal data protection for EU citizens. Although it is not an Indonesia regulation, many e-commerce companies handle customer data in accordance with the GDPR.
- c. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in electronic systems: This regulation covers aspects of personal data protection and provides guidance on the safe management of personal data in electronic systems.
- d. BSI Cybersecurity Framework (BSI-CSF): a cybersecurity framework developed by the British Standards Institution (BSI). It offers guidance on implementing cybersecurity measures in an organization.
- e. Implementation and Security Monitoring of SHA and AES Encryption Algorithms for User Data Applications on Servers: Using these algorithms helps to improve security for personal data protection and system security, making them less vulnerable to hacking attempts.

These regulations and standards play a crucial role in building a solid foundation for ensuring the security and integrity of electronic transactions, especially in the field of e-commerce. Adopting and implementing these measures can contribute significantly to minimizing the risks associated with data breaches and cyber threats.

CONCLUSION

Technological advances must be accompanied by adequate regulations. Over time, technological advancements have led to the emergence of new forms of cybercrime in cyberspace, where individuals can obtain information and engage in cybercrime activities. The existing regulations in Indonesia that currently deal with cybercrime and data breaches appear to have weaknesses or shortcomings as they do not

specifically outline good and appropriate security standards, ensuring that e-commerce users can collectively feel safe and comfortable. Therefore, it is proposed to enact regulations regarding cybercrime and data breaches related to specific and detailed standards for good and decent security. This is aimed at minimizing the occurrence of cybercrime and data breaches.

REFERENCE

- Andriani, N., Jannah, M., Andrianingsih, V. (2022). Key determinants of intention to visit halal tourism in Madura. *al-Uqud: Journal of Islamic Economics*, 6(2), 220–231. <https://doi.org/10.26740/aluqud.v6n2.p220-231>.
- APJII. (2018). Penetration & Behavior Profile of Internet Users in Indonesia. Apjii, 51. Retrieved from www.apjii.or.id. Accessed on November 11, 2023
- Bungin, B. (2011). Qualitative research: communication, economics, public policy, and other social sciences. In Kencana. <https://doi.org/10.1002/jcc.21776>. Accessed on November 11, 2023
- Cholissodin, I. (Brawijaya U., & Riyandan, E. (Brawijaya U. (2018). Big Data Analysis (Theory & Application). *Big Data vs Big Information vs Big Knowledge*, 1.01, 1–476. Accessed from https://www.academia.edu/36718594/Buku_Analisis_Big_Data. Accessed on November 11, 2023
- Dewi Purnama, T., & Alhakim, A. (2021). The importance of the personal data protection law as a form of legal protection for privacy in Indonesia (Vol. 4). <https://fisip.ui.ac.id/bhakti-cybercrime-becomes-type-crime-that-is-experiencing-a-moderate-high-level/>. Accessed on November 11, 2023
- Dewi, O. ;, Teaching Staff, I., Management, J., Polytechnic, I., & Sriwijaya, N. (2011). THE USE OF E-COMMERCE IN THE BUSINESS WORLD.
- Dhianty, R. (n.d.). Privacy Policy and Sectoral Laws and Regulations Digital Platforms vis a vis Personal Data Leakage. *Journal of Public Policy and Law*, 2(1), 186–199.
- House of Representatives of the Republic of Indonesia. (2019). Draft Law of the Republic of Indonesia on Data Protection Personal. (1), 1–41. Accessed from <https://aptika.kominfo.go.id/wpcontent/uploads/2019/09/RUU-PDP.pdf>. Accessed on November 11, 2023
- Firdhy Esterina Christy. (2020). Tempo. <https://data.tempo.co/read/909/prediksiangka-user-e-commerce-diindonesia-2024>. Accessed on November 11, 2023
- Hidayah, A., & Marsitningsih, M. (2020). Legal Aspects of ECommerce Consumer Data Protection. *Cosmic Law*, 20(1), 56. <https://doi.org/10.30595/kosmikhukum.v20i1.8251>. Accessed on November 11, 2023
- Irawan, Aditya Wicaksono, Yusufianto, A., Agustina, D., & Dean, R. (2020). APJII Internet Survey Report 2019 – 2020. Indonesia Internet Service Providers Association, 2020, 1–146. <https://apjii.or.id/survei>. Accessed on November 11, 2023
- Jannah, M. (2021). ZMOT marketing strategy during the Covid-19 pandemic. In *Contemporary Research on Business and Management* (pp. 166-169). CRC Press.
- Kartika Dewi, L., al Azhar Indonesia, U., Masjid Agung Al-Azhar, K., Sisngamangaraja, J., Baru, K., & South, J. (2016). Internet Crime in Electronic Commerce.

- In July Year (Edition 2). <http://cybercrimeandlaw20.blogspot.co.id/2013/0>. Accessed on November 11, 2023
- Kristian Angelo, a, Mary Jovy Anne, V., Azie Trina, M., & Jonathan, C. (2014). Privacy Awareness in E-Commerce. *International Journal of Education and Research*, 2(1). NIST. (2003). NIST Special Publication 800-50. U.S. Department of Commerce.
- Lawrencya, S., Desy, M., & Dewi, P. (2021). Cybercrime as an obstacle to e-commerce in the development of Industry 4.0 based on Indonesia's cultural values.
- Nur, R., Pusklat, R., Cyber, B., & Negara, S. (2022). Cendekia Niaga Journal of Trade Development and Studies Efforts to Build Cybersecurity Awareness in E-commerce Consumers in Indonesia.
- Purnomo, A., Firdaus, M., Hasanah, U., Sno, A.V.D., Prasnowo., M.A. (2021) 'E-Money Academic: Lesson from Literature Visualizing Scientometric Positioning (1968-2019)', *IOP Conference Series: Materials Science and Engineering*, 1071(1), p. 012028. Available at: <https://doi.org/10.1088/1757-899X/1071/1/012028>
- Palinggi, S., Limbongan, E. C., Kharisma Makassar Jl Baji Ateka No, S., Mappakasunggu, B., Makassar, K., & South, S. (2020). The influence of the internet on the e-commerce industry and regulations on the protection of customers' personal data in Indonesia.
- Rahmadi, G., & Rafie Pratama, A. (2020). Analysis of Cyber Security Awareness in the Crowd
- E-Commerce players in Indonesia. *Automata*, 1 (2). <https://journal.uui.ac.id/AUTOMATA/article/view/15399>. Accessed on November 11, 2023
- Ramadhan, H. A., & Putri, D. A. (2018). Big Data, Artificial Intelligence, Blockchain, and Financial Technology in Indonesia. 1–66. Retrieved from <https://aptika.kominfo.go.id/wpcontent/uploads/2018/12/Kajian-KominfoCIPGcompressed.pdf>. Accessed on November 11, 2023
- Safrizal, H. B. A., Eliyana, A., & Gunawan, S. (2020). Spirituality in The Workplace and Employee Performance: A Literature Perspective. *International Journal of Psychosocial Rehabilitation*, 24(7), 880-884.
- University of Indonesia. (2018). The Impact of Cybercrime on Digital Economy Business. <https://www.ui.ac.id/dampak-cybercrime-on-business-digital-economy/>. Accessed on November 11, 2023
- Widagdo, PB (2016). The development of Electronic Commerce (E-Commerce) in Indonesia. *Researchgate.Net*, December, 1–10. <https://www.researchgate.net/publication/311650384>. Accessed on November 11, 2023
- Yanti Liliana, D., Arnanda, R., Ilham Adnan, A., & Hilda Yulastuti, and. (2023). Policy Brief Strengthening the Implementation of Personal Data Protection Regulations for Market Locator Customers in Indonesia (Vol. 2, Issue 1).
- Wantara, P., Suryato T. (2023). Examining Factors Influencing the Online Repurchase Intention. *Transnational Marketing Journal*. Volume: 11, No: 1, pp. 291-310.