International Conference on Economy, Management, and Business (IC-EMBus)
VOL. 1, 2023 p97–104
https://journal.trunojoyo.ac.id/icembus

Regulation of Cyber Security in Online Commerce: Protection Data Protection and Security Threats

Falihatun Nabila[1], Siti Marwa[2], Mochammad Reza Adiyanto[3]
Management Department, Universitas Trunojoyo Madura

INFO ARTIKEL

Keywords:

Cyber Security, Online Commerce,Data Protection, Standardization system

Abstract

Cyber security is an important foundation for the protection of personal data, the development of technology is currently continuous towards 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. But this is inseparable from the possible risks in implementing the system and guaranteeing security. The state plays a role in developing regulations on personal data protection and cybersecurity. The requirement of data protection and strengthening security has not been included in any regulation, making cases of rampant cyber incidents continue to occur due to the absence of established standards. For this reason, it will see how the need to fulfill the requirements of data protection and security guarantees included in a regulation so that all online trading sites and applications can have the right system to protect data and minimize security threats. The author chooses a qualitative method to facilitate data collection obtained through books, journal articles, online media, or library resecrh and other sources. The results show that data protection and security systems are not optimal, and cybersecurity regulations should also apply standardization to realize citizens' rights to their data.

✉ Corresponden Author
(*) Author

Email:
falihatunnabila85@gmail.com[1], sitimarwa1121@gmail.com[2], reza.adiyanto@trunojoyo.ac.id[3]

E-ISSN: 3026-0965

DOI :

INTRODUCTION

Technological developments have affected every aspect of life, including businesses that always have every way of promoting trade in both goods and services to be recognized to a wider scope. In this case, the development that has been carried out in realizing the objectives of promotion is the development of an "Online" trading system or what is often called "ecommerce" to facilitate access to

the trading system over long distances, minimizing the use of paper as a transaction medium and agreement or coordination media.

The rapid growth of the "Online" trading system will also affect the potential risks that will arise. Everything that is managed by the system will have a weak side where it becomes the duty of the state for the incidents that have occurred. Currently, a frequent case is the rampant leakage of customer or e-commerce user data, which is generally due to a negligent or weak security system. The incident has a negative impact on consumers, where consumers are targeted to potentially receive offers of products, services, or information from the seller. In addition, in conducting transactions, consumers are required to register, transact, and pay, which requires input of confidential personal data (Rohmah, 2022). So that potential consumers become victims and as the party who feels the most disadvantaged and rarely satisfactory compensation to overcome the data that has been leaked and has been widespread.

All risks and incidents that occur become the duty of the state in making regulations to reduce data leakage and increase cybersecurity in e-commerce systems. Factually, the government has attempted to form regulations related to cybersecurity 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 (ITE Law), 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 they only cover sanctions for risks that have occurred with the intention of deliberately harming many parties.

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 it is necessary to have regulations that do regulate the improvement of the security system 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 the regulatory arrangements against data leakage and cybersecurity in online trade (e-commerce) in Indonesia? and what solutions can be done in improving the cybersecurity of e-commerce online trade in Indonesia?

LITERATURE REVIEW

1. Cyber Security

Cyber Security comes from the English words "Cyber" and "Security," which are etymologically defined and commonly known as the scope of cyberspace, the internet, or information technology (IT). Cyber Security serves to address, detect, locate, counteract, or minimize the level of risk against disruptions, Cyber threats, and Cyber attacks. In addition, it also includes all cyber technology activities that can threaten the security of all components in the cyber system, 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) offences against the confidentiality, integrity, and availability of computer data and systems; 2) computer-related offences; 3) content-related offences; and 4) copyright-related offences (Siagian et al., 2017).

2. Online Trade (E-commerce)

In the era of globalization marked by rapid advances in information technology, developments are needed in entrepreneurial marketing strategies that are able to reach all consumers in various parts of the world, especially through the use of internet marketing or E-Commerce. Easy access to information provided by internet media is increasing, supported by adequate infrastructure growth (Moor et al., 2009). Rahmanti (2009) Electronic Commerce or ecommerce can be defined as a marketing system that uses electronic media. E-commerce involves the distribution, sale, purchase, marketing, and service of products through an electronic system, such as the internet or in the form of other computer networks. Internet marketing brings five main advantages to companies that adopt it. First, both large and small companies can implement it. Second, there are no physical limitations in 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 at any time. Fifth, the buying process can be done more quickly and independently (Kotler in Widodo, 2002).

3. Data Protection

Protection of personal data is considered part of the effort to protect human rights. Therefore, arrangements relating to privacy rights related to personal data are a form of recognition and protection of basic human rights. In the context of international relations, Indonesia is expected to meet the demands for the protection of personal data and information, which can support the smooth running of trade, industry and investment with a transnational nature (Hukum, 2020).

RESEARCH METHODS

The method applied in this research is qualitative descriptive method. Sugiyono (2016) asserts that qualitative research method is used to investigate the natural conditions of the object, where the researcher acts as the main instrument. Nazir (2014) explains that descriptive research focuses on analyzing the status of human groups, objects, conditions, thought systems, or current events with the aim of producing systematic, factual, and accurate descriptions of the facts being studied. Sukmadinata (2011:73) mentions that qualitative descriptive research aims to explain and describe existing phenomena, whether natural or human-engineered, with an emphasis on characteristics, qualities, and interrelationships among activities.

This research is conducted with the purpose of collecting current and detailed information, identifying problems, making comparisons or evaluations, and determining the steps taken by others in facing similar problems, with the hope of learning from their experiences to plan and make decisions in the future. Thus, qualitative descriptive research only focuses on describing responses to situations, events, or phenomena that occur, without requiring explanations of causal relationships or hypothesis testing.

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

interpretation process is carried out from the researcher's perspective (Diantha, 2017).

RESULT AND DISCUSSION

In tandem 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 desires and needs of its users. One technological advancement or convenience for internet users is the access to e-commerce. The process of buying and selling, which was previously limited to conventional methods, can now be conducted electronically through internet platforms. 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 saw an increase of only 158.65 million users. Looking at the current trend, e-commerce users in Indonesia continue to grow, with the projected number expected to reach 196.47 million users by the end of 2023. This figure is anticipated to continue increasing in the next four years.

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

According to the scientific journal "Pemanfaatan E-commerce dalam Dunia Bisnis" (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 transactions or exchanging products and services conducted 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, recruitment of labor, and insurance.

The conveniences experienced across various sectors are not exempt from the possibility of risks in the implementation of systems and security assurances. The state plays a crucial role in creating regulations for the protection of personal data and cyber security. In Indonesia, the government has adopted several regulations related to cyber security and personal data protection in the context of e-commerce. These regulations aim to protect consumers, companies, and personal data from the potential risks of data leaks and misuse. There are several regulations governing cyber security and data protection in Indonesia, including:

a. Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law). This law serves as a legal framework encompassing legal and criminal aspects in the use of information technology, including online trade or e-commerce. In the context of e-commerce, the ITE Law provides a legal basis for all actions against cybercrimes, including data breaches. On April 29, 2008, this law was enacted as Indonesia's first cyber law.

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 aspects of cyber security 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 the protection of personal data.

d. Minister of Communication and Information Regulation 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. It requires the processing of 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 cyber security and personal data, there are also consumer protection aspects in the applicable consumer laws in Indonesia. This protection includes consumer rights to privacy and the security of users' personal information.

The regulations established by the state or government mentioned above serve as a legal foundation to involve e-commerce managers in maintaining cybersecurity and data protection. However, law remains law, and regulations remain regulations, each having inherent weaknesses in their implementation. For instance, in the ITE Law, which became Indonesia's first cyber law. Despite the comprehensive regulations within the Law on Electronic Information and Transactions concerning cybercrimes and data breaches, some articles are deemed insufficiently specific in addressing these issues. This may complicate the enforcement of the law in the continually evolving cybersecurity landscape.

Moreover, certain provisions in the Law on Electronic Information and Transactions impose seemingly severe penalties, including lengthy imprisonment terms and substantial fines. This could instill excessive fear and elevate the risk of legal misuse. While there are regulations related to personal data protection, the primary focus of the Law on Electronic Information and Transactions is on cybercrimes in general. This might result in less detailed and less stringent regulations for personal data protection. Some terms in this law are also ambiguously defined, leading to diverse interpretations and legal uncertainty, particularly when handling cases of cybercrimes and data breaches.

Unbeknownst, due to the rapid pace of technological advancement, the Law on Electronic Information and Transactions may not promptly accommodate emerging issues in the cybersecurity realm. This creates legal loopholes or an inability to swiftly respond to new threats. It can also be argued that the Law on Electronic Information and Transactions is inadequate in providing clear and focused guidelines or regulations on a company's obligation to report cybersecurity incidents to relevant authorities or affected parties.

Laws and regulations are not static entities; they continuously evolve with the progress of time and technology. This applies to regulations governing cybercrimes and data breaches. Despite existing regulations such as the Law on Electronic Information and Transactions and the aforementioned ones, the legal landscape in

Indonesia cannot turn a blind eye to the onthe-ground reality that shows the adverse consequences of rapid technological advancement. This has led to irresponsible individuals becoming increasingly adept at exploiting existing regulations.

Within existing regulations or laws, there is a lack of specificity in detailing the standards for good and proper security, thereby minimizing the likelihood of data breaches and cybercrimes. Nevertheless, to prevent data leaks and safeguard information, especially in the context of online commerce (e-commerce), there are several regulations and security standards that could 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): a European Union regulation that provides personal data protection for EU citizens. While not an Indonesian regulation, many e-commerce companies handle customer data in accordance with GDPR.
c. Minister of Communication and Information Regulation Number 20 of 2016 on the Protection of Personal Data in electronic systems: this regulation covers aspects of personal data protection and provides guidance on secure management of personal data in electronic systems.
d. BSI Cyber Security Framework (BSI-CSF): a cybersecurity framework developed by the British Standards Institution (BSI). It offers guidance on implementing cybersecurity measures within an organization.
e. Implementation and Monitoring of SHA and AES Encryption Algorithm Security for User Data Applications on Servers: Using these algorithms helps enhance security for the protection of personal data and system security, making it less susceptible to hacking attempts.

These regulations and standards play a crucial role in establishing a robust foundation for ensuring the security and integrity of electronic transactions, particularly in the field of ecommerce. Adopting and implementing these measures can contribute significantly to minimizing the risks associated with data breaches and cyber threats.

CONCLUSION

The advancement of technology must be accompanied by adequate regulations. Over time, technological progress has led to the emergence of new forms of cybercrime in the virtual world, where individuals can acquire information and engage in cybercriminal activities. Existing regulations in Indonesia that currently address cybercrime and data breaches appear to have weaknesses or deficiencies as they do not specifically elaborate on the standards for good and proper security, ensuring that e-commerce users can collectively experience security and comfort. Therefore, it is proposed to enact regulations concerning cybercrime and data breaches related to specific and detailed standards for good and proper security. This is aimed at minimizing the occurrence of cybercrime and data breaches.

REFERENCE

APJII. (2018). Penetrasi & Profil Perilaku Pengguna Internet Indonesia. Apjii, 51. Retrieved from www.apjii.or.id. Diakses pada 11 November 2023

Bungin, B. (2011). Penelitian Kualitatif: Komunikasi, Ekonomi, Kebijakan Publik, Dan Ilmu Sosial Lainnya. In Kencana. https://doi.org/10.1002/jcc.21776. Diakses pada 11 November 2023

Cholissodin, I. (Brawijaya U., & Riyandan, E. (Brawijaya U. (2018). Analisis Big Data (Teori & Aplikasi). Big Data vs Big Information vs Big Knowledge, 1.01, 1–476. Retrieved from https://www.academia.edu/36718594/Buku_Analisis_Big_Data. Diakses pada 11 November 2023

Dewi Purnama, T., & Alhakim, A. (2021). Pentingnya uu perlindungan data pribadi sebagai bentuk perlindungan hukum terhadap privasi di Indonesia (Vol. 4). https://fisip.ui.ac.id/bhakti-cybercrime-menjadi-jenis-kejahatan-yangmengalami-peningkatan-cukup-tinggi/. Diakses pada 11 November 2023

Dewi, O. :, Staf Pengajar, I., Manajemen, J., Politeknik, I., & Sriwijaya, N. (2011). PEMANFAATAN E-COMMERCE DALAM DUNIA BISNIS.

Dhianty, R. (n.d.). Kebijakan Privasi (Privacy Policy) dan Peraturan Perundang-undangan Sektoral Platform Digital vis a vis Kebocoran Data Pribadi. Jurnal Kebijakan Publik Dan Hukum, 2(1), 186–199.

DPR RI. (2019). Rancangan Undang-Undang Republik Indonesia Tentang Perlindungan Data

Pribadi. (1), 1–41. Retrieved from https://aptika.kominfo.go.id/wpcontent/uploads/2019/09/RUU-PDP.pdf. Diakses pada 11 November 2023

Firdhy Esterina Christy. (2020). Tempo. https://data.tempo.co/read/909/prediksiangkapengguna-e-commerce-diindonesia-2024. Diakses pada 11 November 2023

Hidayah, A., & Marsitiningsih, M. (2020). Aspek Hukum Perlindungan Data Konsumen ECommerce. Kosmik Hukum, 20(1), 56. https://doi.org/10.30595/kosmikhukum.v20i1.8251. Diakses pada 11 November 2023

Irawan, aditya wicaksono, Yusufianto, A., Agustina, D., & Dean, R. (2020). Laporan Surve Internet APJII 2019 – 2020. Asosiasi Penyelenggara Jasa Internet Indonesia, 2020, 1–146. https://apjii.or.id/survei. Diakses pada 11 November 2023

Kartika Dewi, L., al Azhar Indonesia, U., Masjid Agung Al-Azhar, K., Sisingamangaraja, J., Baru, K., & Selatan, J. (2016). Internet Crime Dalam Perdagangan Elektronik.

In Juli Tahun (Issue 2). http://cybercrimeandlaw20.blogspot.co.id/2013/0. Diakses pada 11 November 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). Kejahatan Siber Sebagai Penghambat E-Commerce Dalam Perkembangan Industri 4.0 Berdasarkan Nilai Budaya Indonesia.

Nur, R., Pusdiklat, R., Siber, B., & Negara, S. (2022). Cendekia Niaga Journal of Trade Development and Studies Upaya Membangun Kesadaran Keamanan Siber pada Konsumen E-commerce di Indonesia.

Palinggi, S., Limbongan, E. C., Kharisma Makassar Jl Baji Ateka No, S., Mappakasunggu, B.,

Makassar, K., & Selatan, S. (2020). Pengaruh Internet Terhadap Industri Ecommerce Dan Regulasi Perlindungan Data Pribadi Pelanggan Di Indonesia.

Rahmadi, G., & Raf'ie Pratama, A. (2020). Analisis Kesadaran Cyber Security pada Kalangan

Pelaku e-Commerce di Indonesia. Automata, 1 (2). https://journal.uii.ac.id/AUTOMATA/article/view/15399. Diakses pada 11 November 2023

Ramadhan, H. A., & Putri, D. A. (2018). Big Data, Kecerdasan Buatan, Blockchain, dan Teknologi Finansial di Indonesia. 1–66. Retrieved from https://aptika.kominfo.go.id/wpcontent/uploads/2018/12/Kajian-KominfoCIPGcompressed.pdf. Diakses pada 11 November 2023

Universitas Indonesia. (2018). Dampak Kejahatan Siber Pada Bisnis Ekonomi Digital. https://www.ui.ac.id/dampak-kejahatan-siber-pada-bisnis-ekonomi-digital/. Diakses pada 11 November 2023

Widagdo, P. B. (2016). Perkembangan Electronic Commerce (E-Commerce) di Indonesia. Researchgate.Net, December, 1–10. https://www.researchgate.net/publication/311650384. Diakses pada 11 November 2023

Yanti Liliana, D., Arnanda, R., Ilham Adnan, A., & Hilda Yuliastuti, dan. (2023). Policy BriefPenguatan Implementasi Regulasi Perlindungan Data Pribadi Bagi Pelanggan Lokapasar di Indonesia (Vol. 2, Issue 1).