Journal Of Economics, Technology, and Business (JETBIS)
Volume 3, Number 8 August 2024
p-ISSN 2964-903X; e-ISSN 2962-9330

CONSUMER DATA PROTECTION IN ELECTRONIC TRANSACTION PRACTICES IN E-COMMERCE

Alikhan Salim[1], Tri Susilowati[2], Hono Sejati[3]
Universitas Darul Ulum Islamic Centre Sudirman GUPPI, Indonesia
Email: alikhansalim00@gmail.com[1], tri.susilowati.undaris@gmail.com[2], sejatihono@gmail.com[3]

KEYWORDS:
Marketplace; Consumer Data; Consumer Protection.

ABSTRACT

Online transactions provide huge benefits for buyers and sellers. For buyers, the convenience of shopping without having to go to a physical store is the main benefit. They can compare prices and products from various sellers, saving time and transportation costs. For sellers, online transactions open up wider market opportunities, increase product exposure, and increase sales and distribution efficiency. However, the risk of personal data leakage always lurks in online transactions. This issue is serious and can compromise consumers' privacy and information security. Data leaks can occur when personal information such as names, addresses, telephone numbers, emails, credit card details and other personal data falls into unauthorized hands. The research aims to explore the protection of consumers' personal data and examine the responsibility of marketplaces in dealing with data leaks. The author uses a normative juridical approach, which includes primary and secondary legal analysis, as well as descriptive analysis to summarize applicable regulations and legal theory related to practice. The results show that Indonesia has Law Number 27 of 2022 concerning Protection of Consumer Personal Data to protect personal data. Marketplaces that violate these rules may be subject to administrative sanctions in accordance with applicable regulations, while consumers have the right to file a lawsuit for marketplace negligence in accordance with Article 1366 of the Civil Code.

INTRODUCTION

Electronic commerce, or E-commerce, has grown rapidly since the early 1990s, fundamentally changing the way we shop and do business. Its history can be traced back to the 1960s when organizations started using Electronic Data Interchange (EDI) for the electronic exchange of business documents. E-commerce as we know it today began to emerge in the 1990s along with the development of the World Wide Web (www). Amazon, founded in 1994 by Jeff Bezos, became one of the successful pioneers of E-commerce with its innovative online bookstore concept. Although E-commerce experienced significant growth in the late 1990s and early 2000s, there are still concerns about the security of online transactions among consumers. The existence of e-commerce in the last two decades has been driven by a number of various factors, including:

a. Advancement in Internet Infrastructure: Expanding reach of the internet and increasing its speed globally has eased access to E-commerce platforms, accelerating its growth.

b. Increased Consumer Confidence: Online transaction security measures and better customer service have strengthened consumer confidence in E-commerce. Testimonials and reviews from previous customers also play an important role in building trust.
c. Convenience and Consumer Satisfaction: E-commerce offers the convenience of 24/7 shopping from multiple locations, while presenting a variety of products and services that can be tailored to consumer preferences.
d. Mobile Device Penetration: The emergence of smartphones and tablets has changed the way consumers interact with E-commerce. Transactions via mobile devices or mobile commerce are becoming one of the main trends in this industry.

As E-commerce has developed, this industry has experienced quite striking segmentation and diversification. In the beginning, E-commerce mainly focused on selling physical products such as books, electronics and clothing. However, over time, E-commerce has expanded its reach into various sectors, including travel (booking plane tickets and hotels), food and beverage (food delivery), entertainment (streaming music and films), and many more. The current development of e-commerce is closely related to innovation and technological breakthroughs. Some of the innovations that have changed the face of E-commerce include:

a. Artificial Intelligence (AI): AI has been applied in E-commerce to provide a more personalized shopping experience, increase product search accuracy and improve customer service.
b. Augmented Reality (AR) and Virtual Reality (VR): AR and VR have been utilized to enhance the online shopping experience by providing a more realistic visual representation of the product and its features.
c. Internet of Things (IoT): IoT has integrated smart home devices with E-commerce, allowing consumers to automate purchases based on their needs.

In today's era, E-commerce has become an integral part of the digital revolution. Many large E-commerce companies have experienced rapid growth and dominated the market globally. Additionally, E-commerce has provided opportunities for many small and medium scale businesses to achieve success through their online platforms. E-commerce has become an important component of the sharing economy, where platforms such as Airbnb and Gojek provide online-based transportation and accommodation services that are changing the way people access these services. However, on the other hand, E-commerce still faces a number of challenges, including increasing transaction security, overcoming logistics and delivery problems, and increasing consumer protection.

In E-commerce, consumer data leakage is a serious problem that often occurs, threatening privacy and security. Examples of incidents include the eBay data leak in 2014 (145 million accounts affected), Target in 2013 (40 million customers affected), Ashley Madison in 2015 (37 million accounts affected), Home Depot in 2014 (56 million customers affected), and the Cambridge scandal Analytica-Facebook in 2018. This highlights the need for better data protection in E-commerce. Meanwhile, in 2020, there was a leak of consumer personal data in Indonesia via the Bukalapak e-commerce site. Around 13 million Bukalapak user accounts were affected, with information such as full names, email addresses, telephone numbers and

shipping addresses spread across online dark forums. Although account passwords are not affected, the potential misuse of personal data remains a serious threat to users.

This incident raises concerns about data security and customer privacy in Indonesian E-commerce. Bukalapak has taken steps to warn users and strengthen their security systems, emphasizing the importance for E-commerce companies to increase data protection. This includes investment in advanced security systems, staff training, and transparency to customers. Consumers also need to be aware of security threats, check site security protocols and use unique passwords to protect their data.

The research is focused on exploring the protection of consumers' personal data, particularly in the context of digital marketplaces. It seeks to understand the measures in place to safeguard this sensitive information and to assess the responsibilities that marketplaces have when it comes to handling data breaches. By examining how these entities respond to data leaks, the study aims to provide insights into the effectiveness of current protections and identify areas where improvements may be necessary to ensure consumer trust and data security.

Referring to the context mentioned previously, the author is interested in conducting research or analysis on how to protect consumer personal data in the marketplace in accordance with applicable law. This article will reveal in detail the answers to two main questions: how is consumer personal data protected in e-commerce transactions according to applicable laws and regulations and what is the marketplace's responsibility for leaks of consumer personal data.

RESEARCH METHODS

The research on safeguarding consumer personal data during E-commerce transactions in Indonesia adopts a qualitative and normative juridical approach. To address research objectives, the study uses a literature review method that scrutinizes primary, secondary, and tertiary legal materials. Primary legal material is mainly statutory regulations (Soekanto, 2007), whereas secondary legal materials include academic journals, books, official reports, opinions, and more. Tertiary legal materials, such as dictionaries and encyclopedias, are also studied. This research employs analytical techniques to interpret norms and contextualize provisions to their practical application in the field, drawing correlations with the PDP Law.

RESULTS AND DISCUSSION

Consumer Personal Data Protection Regulations in E-commerce Transactions

In the increasingly widespread era of the internet and social media, protecting consumer personal data is becoming increasingly important. Data such as names, addresses, phone numbers, and others collected by platforms and services have great value. While it is common for businesses to collect data, it's important to consider the potential risks of leaks or security breaches. These threats can lead to serious consequences such as identity theft, fraud, and financial and reputational damage. To safeguard privacy, security, and consumer rights, E-commerce platforms have implemented personal data protection measures.

According to Isnaeni (Isnaeni, 2018), legal protection can be divided into internal and external protection. Internal protection occurs when both parties have a balanced legal position and can formulate an agreement according to their respective interests. Meanwhile, external

protection, imposed by the authorities through regulations, aims to protect the interests of weaker parties. In principle, regulations must be fair and provide balanced protection to all parties. It is important to prevent imbalances that harm one party, such as when debtors violate creditor rights. Therefore, regulations must be designed to provide proportional protection to all involved. Legal protection involves efforts to protect individuals or entities as legal subjects through regulations and law enforcement with the threat of sanctions. Muchsin divides legal protection into two types: preventive and repressive (Muchsin, 2003). Preventive protection, according to him, aims to prevent violations before they occur, usually through regulations that set limits and procedures to minimize risks, as well as providing space for input from legal subjects before a final decision is taken. This not only reduces conflict but also encourages governments to act more carefully and consider decisions carefully.

Meanwhile, CST Kansil explained that repressive legal protection includes sanctions such as fines and imprisonment after violations occur, aimed at resolving conflicts (Kansil, 1979). It includes law enforcement by the General and Administrative Courts. The basic principles in legal protection against government actions involve the recognition and protection of human rights, as well as the principle of the rule of law which emphasizes the protection of human rights in the context of the goals of the rule of law. Legal protection aims to guarantee every citizen's rights that are being disturbed. It is the foundation for a just legal system and provides a framework for resolving disputes, protecting individual rights, and maintaining societal order. The purpose is to prevent the government and authorities from committing abuses against citizens. Legal protection includes transparent legal processes, equal access to courts, and fair application of the law to all individuals without exception.

Legislation has a crucial role in protecting consumer personal data. In Indonesia, the right to protection of personal data is officially recognized in the 1945 Constitution of the Republic of Indonesia. Constitutional Court Decision Number 20/PUU-XIV/2016 strengthens this protection as part of individual privacy rights. Data protection and privacy, although related, are different concepts. Personal data protection is considered a human right and is strengthened by international legal treaties. The government has a central role in establishing policies that ensure optimal protection of consumers' data, especially in the context of registration on E-commerce platforms (Pohan & Nasution, 2023).

The public needs to be given an equal understanding of the importance of protecting personal data or the privacy rights they have. The state has a responsibility to provide equal education for all its citizens in this regard. Lack of protection of privacy rights can threaten, both a person's physical safety and assets. Apart from providing education, Indonesia is also obliged to provide legal protection to its citizens by the principles of Pancasila (Rizal, 2019). Initially, in Indonesia, there were no special regulations that explicitly regulated the protection of personal data. The protection is only generally covered by several different laws, such as the ITE Law, Archives Law, Company Documents Law, Banking Law, Health Law, Telecommunications Law, and Population Administration Law. Apart from that, some laws specifically protect consumer rights, such as the Consumer Protection Law.

In 2022, Indonesia issued Law Number 27 of 2022 concerning Personal Data Protection (UU PDP). This law was designed to respond to the need for individual privacy and personal data security in the ever-evolving digital era. Rapid developments in information and

communication technology are the main background for the creation of this regulation, considering changes in the way personal data is collected, stored, processed, and transferred. It is hoped that regulations regarding personal data protection will put Indonesia on par with developed countries that already have similar laws. It is hoped that this step will strengthen Indonesia's position as a trusted business center, which is an important strategy in the national economy (Rizal, 2019). One of the important foundations in supporting the protection of personal data is Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), which has undergone revision through Law Number 19 of 2016. The ITE Law provides a legal framework to protect individual privacy in a digital context and establish sanctions for misuse of data. Article 25 and Article 26 of the ITE Law specifically regulate the protection of personal data in electronic transactions.

Article 25 of the ITE Law confirms that all intellectual works created in the form of electronic information, electronic documents, or websites, are protected as Intellectual Property Rights by applicable regulations. Article 26 of the ITE Law also emphasizes that the use of personal data in the context of electronic media requires permission from the owner of the relevant data. Violation of this provision may result in claims for resulting losses (Ramadaani & Muaalifin, 2023). Article 26 of the ITE Law explains that personal data is part of individual rights regarding privacy. In the context of the use of Information Technology, personal data protection is an inseparable part of privacy rights. Privacy rights include the right to enjoy one's private life without interference, The right to communicate with others without being intercepted, and The right to control access to information about one's private life and personal data (Dewi, 2016).

Overall, the ITE Law regulates the protection of personal data in Chapter VII, especially Articles 30-33 and Article 35. This law prohibits illegal access to personal data through electronic systems and states that wiretapping may only be performed by authorities in the context of law enforcement. Breach of this may result in a claim for damages, with the perpetrator responsible for his or her actions (Anggriawan, 2023). Although the ITE Law provides protection, the definition of personal data is not explained in detail but can be found in other related regulations such as PP 71/2019 and Minister of Communication and Information Technology Regulation Number 20 of 2016. The PDP Law, for example, defines personal data into two main categories: specific (such as health and biometric data) and general (such as full name and gender).

Personal Data Protection includes standards to protect personal data, whether processed electronically or non-electronically, with flexibility to apply according to sector needs. The aim is to protect citizens' privacy, ensure good public services, support digital economic growth, and increase the competitiveness of domestic industry. Government Regulation Number 80 of 2019 concerning Trading via Electronic Systems (PP PMSE) also regulates the protection of personal data in E-commerce transactions, especially in Articles 58-59. Article 58 PP PMSE stipulates that personal data is treated as the personal property of the individual or company involved. Business actors who receive personal data are required to act as data custodians by applicable regulations.

Articles 58-59 of PP PMSE stipulate the responsibility of business actors in managing people's data without providing guidelines regarding sanctions or obligations if there is a violation in the protection of personal data. From a legal perspective, the concept of personal

data as property rights emphasizes that individuals or business actors have full control over their data, including the right to grant or refuse permission for the use and disclosure of that data by other parties. Recognition of personal data as property can ensure the privacy and security of individual or business information. This property rights principle also encourages the protection of the ownership rights of individuals or business actors over their data, so that other parties cannot use the data without permission or for a legitimate purpose.

Protection of Consumer Personal Data in Electronic Transactions is also regulated in the Minister of Communication and Information Technology Regulation Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems (Kominfo Regulation 20/2016). The implementation of the electronic system considers the protection of consumers' data through the establishment of a code of ethics in the form of a self-regulation policy. For companies involved in electronic commerce, the preparation of privacy policies as part of self-regulation is a potential solution in dealing with the problem of protecting consumer personal data. This is in line with the mandate of Article 5 paragraph (2) of Kominfo Regulation 20/2016 which emphasizes the need for every electronic system operator to have internal regulations for personal data protection as a preventive measure to prevent data leaks (Ramadaani & Muaalifin, 2023).

Before the ITE Law and PDP Law, the state had protected consumers through the 1999 PK Law. This law stipulates consumer rights and responsibilities. One of the rights is "the right to enjoy comfort, security, and safety when using goods and/or services." (Indonesia, 1999)In the context of buying and selling transactions, consumers have the right to comfort and security of their data, by what is regulated in the PK Law. Article 7 of the PK Law also emphasizes the obligations of business actors, including the obligation to act in good faith. It means that if before an electronic transaction occurs, the seller asks for personal data such as address or telephone number, the seller has a moral obligation to maintain the confidentiality of consumers' data in good faith and not use it for bad interests (Aryani & Susanti, 2022).

If consumers experience losses, they have the right to file a lawsuit by the provisions of Article 45 of the PK Law. This article allows consumers who have suffered losses to file a lawsuit against business actors through consumer dispute resolution institutions or courts in the general court environment. In resolving disputes, consumers have the option to choose between resolving in court or through alternative channels outside of court. For example, when personal data leaked on the Tokopedia platform, David Tobing filed a lawsuit because he felt that the Ministry of Communication and Information had failed to supervise Tokopedia's implementation of the electronic system, which resulted in Tokopedia users' data being accessed illegally by irresponsible parties (Charos et al., 2023).

a. Marketplace Liability for Consumer Personal Data

Marketplaces have a great responsibility towards consumers to ensure the protection of their rights and interests in E-commerce transactions. As an online platform that connects sellers and consumers, market places play an important role in providing a safe and trustworthy environment. Some of the responsibilities of market places towards consumers include:

a. Personal Data Protection: Marketplaces must maintain the security and confidentiality of the personal data of consumers registered on its platform, and ensure that the use of such data is in accordance with applicable regulations.
b. Seller and Product Verification: Marketplaces are responsible for ensuring the credibility of sellers and the quality of products offered, as well as removing sellers who engage in fraudulent practices or the sale of counterfeit products.
c. Information Transparency: Marketplaces must provide clear and accurate information about the products or services offered, including prices, product descriptions, delivery terms, and return policies.
d. Dispute Handling: Marketplaces should have an effective dispute resolution mechanism between consumers and sellers, and act as a mediator in finding a fair solution for both parties.
e. Return Policy and Quality Assurance: Marketplaces should have a fair return policy for consumers if the product or service does not meet expectations, and guarantee the quality of the product or service offered.
f. Protection against Fraudulent Practices: Marketplaces should be proactive in fighting fraudulent practices and counterfeit products, and remove sellers who engage in such practices from the platform.
g. Consumer Education: Marketplaces have a responsibility to educate consumers about their rights and obligations in online transactions, including how to protect themselves from fraud and their rights in E-commerce.

Broadly speaking, liability refers to the obligation to face the consequences of one's actions. In a legal context, liability refers to the responsibility of a person or group for actions that violate the law. According to the definition in the legal dictionary, liability refers to a person's obligation to fulfill what has been required of him with full responsibility." (Hamzah, 1986) According to Hans Kelsen, a leading Austrian legal expert and philosopher of law, in the legal realm, liability is based on the applicable legal norms, stating that a person is legally responsible for his actions. In the case of consumer personal data leaks, there are several principles of liability that can be applied to marketplace platforms, including:

a) The fault-based principle, which refers to an element that is contrary to the law, which includes the moral and ethical requirements of society. This principle requires proof that there is a connection between the fault and the harm caused.
b) The presumption of liability, which states that the party who is the defendant is assumed to be liable unless he can prove his innocence. This principle is also known as the reverse proof system (Shidarta, 2006). The use of the presumption of liability construction can be considered relevant when data leakage occurs due to unforeseen circumstances or negligence on the part of the online marketplace.
c) The Principle of Absolute Liability states that the party causing the loss is always responsible, regardless of fault or who is at fault (Muthiah, 2016). In Sidharta's perspective, Strict liability is a characteristic of tort actions that places direct responsibility on the business actor without the need to prove fault (Muthiah, 2016). In this principle, the marketplace is not required to be responsible for the leakage of consumer personal data if the leakage is caused by force majeure. This view is in line with some experts who consider

strict liability as an obligation without requiring proof of fault, except in unavoidable situations (Priliasari, 2023)."

Article 15 of the ITE Law confirms that Electronic System Operators must run their systems reliably and securely, and take full responsibility for their functionality. However, this provision does not apply if the marketplace can prove force majeure or user error of the electronic system. Personal data leaks in marketplaces show weaknesses in their security systems, which allow access to consumer data by unauthorized parties. This violates the provisions of Article 15 of the ITE Law and Article 3 of PP PSE which require Electronic System Providers to organize their systems reliably and securely. Thus, the responsibility for the leakage of personal data of marketplace users will be the responsibility of the marketplace organizer (Indriyani, 2017).

Based on Government Regulation No. 71/2019 on the Implementation of Electronic Systems and Transactions (PP 71/2019), Electronic System Operators are responsible for protecting users and the public from the risks of the systems they operate. They must ensure the confidentiality, integrity and availability of information in accordance with the law. Article 14 paragraph (5) of PP 71/2019 requires written notification if there is a failure to protect personal data. If there is a hack of the server that stores personal data, the organizers must notify the affected parties. Therefore, they must secure the stored data. In addition, it is necessary to educate staff responsible for infrastructure security and protection, including ensuring the security of computer programs containing individuals' personal data (Kurniawan et al., 2022).

The PDP Law further establishes obligations for the Controller of personal data, which refers to the individual, public body or international organization that sets the purpose and controls the processing of Personal Data. Personal data controllers can come from the government sector, such as the Directorate General of Population and Civil Registration, Ministry of Home Affairs, which collects personal data of residents for the benefit of the state. On the other hand, private companies, such as marketplaces, also act as personal data controllers, as they ask users to provide personal data as a condition for using the services they offer."

Article 35 of the PDP Law emphasizes that Personal Data Controllers must safeguard and guarantee the security of the Personal Data they process. They should use technical and operational measures to protect Personal Data from unauthorized use, in accordance with the law and taking into account the level of risk associated with the Personal Data they handle. Furthermore, Article 39 of the PDP Law provides that Personal Data Controllers shall prevent unauthorized access to Personal Data by using reliable, secure, and responsible security systems, in accordance with applicable regulations. Article 46(1) stipulates that in the event of a Personal Data leak, the Personal Data Controller must notify the Personal Data Subject and relevant institutions within 3 x 24 hours. The notification must at least include information about the Personal Data disclosed, the time and manner in which the Personal Data was disclosed, and the measures taken to handle and recover the disclosed Personal Data (Nirwana, 2023).

According to the regulations mentioned above, marketplaces have the responsibility to keep personal data secure. However, in the event of a security breach that results in a personal

data leak, the marketplace acting as the controller of the personal data must notify the consumers affected by the hack. In addition, marketplaces may be subject to administrative sanctions such as written warnings, temporary suspension of personal data processing, deletion or destruction of personal data, and/or administrative fines in accordance with Article 57 of the PDP Law. Likewise, according to the provisions in PP 71/2019, electronic system providers can also be subject to sanctions such as written warnings, administrative fines, temporary suspension, termination of access, and/or license revocation."

In the event of a violation of the confidentiality of consumer personal data, consumers have the right to file a complaint with the Minister regarding the failure of personal data protection, as stipulated in Article 26 letter b. This relates to the right of data owners to complain to the Minister regarding the failure of personal data protection. In addition, consumers who feel aggrieved can claim civil compensation from the marketplace for negligence committed by the marketplace. In terms of negligence, Article 1336 of the Civil Code states that individuals are liable not only for their actions, but also for losses caused by their negligence or recklessness. Article 1366 of the Civil Code encompasses the idea that a person can be held legally responsible not only for the wrongs they commit, but also for their negligence that causes harm to others. On the other hand, according to Article 64 of the PDP Law, dispute resolution can be done through several means, such as arbitration, courts, or alternative dispute resolution institutions, using legal procedures in accordance with applicable regulations and with valid evidence.

CONCLUSION

Prior to 2022, personal data protection regulations were scattered across several laws, but now Indonesia has a law that specifically regulates personal data protection. The protection of E-commerce consumer rights has become crucial in Indonesia as the issue of personal data has become a serious problem that needs to be resolved immediately. The many cases of personal data leakage on E-commerce platforms in Indonesia pose a big threat to the Government if the rights of E-commerce consumers are not properly protected. In the case of consumer personal data leakage, the marketplace is responsible for the losses suffered by consumers as data owners. Consumers also have the right to file a lawsuit for compensation against the marketplace on the basis of negligence based on Article 1366 of the Civil Code. Law No. 27 of 2022 on Personal Data Protection requires the establishment of a personal data protection supervisory institution. This institution has a crucial role in overseeing the implementation of personal data protection. This institution is also a channel for consumers to convey their aspirations regarding personal data protection. Given the important role of this institution, the Government must immediately establish an independent institution. In addition, to increase awareness of the importance of protecting personal data, the public needs to be given adequate digital literacy education.

BIBLIOGRAPHY

Anggriawan, Z. (2023). Analisis Perlindungan Hukum terhadap Data Konsumen Marketplace di Indonesia Berdasarkan Undang-undang No 27 Tahun 2022. *Humaniorum*, *1*(02).

Aryani, A. P., & Susanti, L. E. (2022). Pentingnya Perlindungan Data Pribadi Konsumen dalam Transaksi Online pada Marketplace terhadap Kepuasan Konsumen. *Ahmad Dahlan Legal*

Perspective, *2*(1).
Charos, W. A., Irwan, M., Nasution, P., Dan, F. E., & Islam, B. (2023). Perlindungan Privasi Dan Data Pribadi Konsumen Pada E-Commerce. *Jurnal Akuntansi Keuangan Dan Bisnis*, *1*(2).
Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, *5*(1).
Hamzah, A. (1986). Kamus hukum.
Indonesia, R. (1999). Undang-Undang No. 8 tahun 1999 tentang perlindungan konsumen. *Lembaran Negara RI Tahun*, *8*.
Indriyani, M. (2017). Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System. *Justitia Jurnal Hukum*, *1*(2).
Isnaeni, M. (2018). Seberkas Diorama Hukum Kontrak. *Surabaya: Revka Petra Media*.
Kansil, C. S. T. (1979). Pengantar Ilmu Hukum Dan Tata Hukum Indonesia.
Kurniawan, I. G. H., Olivia, F., Judge, Z., Siswanto, A. H., Suprayogi, A., & Slamet, S. R. (2022). Penyuluhan Aspek Hukum Perlindungan Privasi Dan Data Pribadi. *Jurnal Abdimas*, *08*(05).
Muchsin, M. (2003). Perlindungan dan Kepastian Hukum bagi Investor di Indonesia. *Universitas Sebelas Maret*.
Muthiah, A. (2016). Tanggung Jawab Pelaku Usaha kepada Konsumen tentang Keamanan Pangan dalam Perspektif Hukum Perlindungan Konsumen. *Dialogia Iuridica*, *7*(2), 1–23.
Nirwana, M. A. (2023). Perlindungan Hukum Terhadap Data Pribadi Sebagai Hak Privasi Individual. *Al Wasath Jurnal Ilmu Hukum*, *3*(2).
Pohan, T. D., & Nasution, M. I. P. (2023). Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce. *Sammajiva: Jurnal Penelitian Bisnis Dan Manajemen*, *1*(3), 42–48.
Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(2).
Ramadaani, K. F., & Muaalifin, M. D. A. (2023). Analisis Yuridis Pengaturan Hak Untuk Dilupakan (Right To Be Forgotten) Dalam Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. *Legacy: Jurnal Hukum Dan Perundang-Undangan*, *3*(1), 18–41.
Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum*, *10*(2), 218–227.
Shidarta, S. (2006). Pemetaan kelembagaan perlindungan konsumen. *Jurnal Hukum Pro Justitia*, *24*(1).
Soekanto, S. (2007). *Penelitian hukum normatif: Suatu tinjauan singkat*.