INTERNATIONAL CONFERENCE ON THE STATE, LAW, POLITICS & DEMOCRACY (ICON-SLPD)
P-ISSN : 2962-7109 E-ISSN : 3063-6957
https://openjournal.unpam.ac.id/index.php/ICon

International Conference On The State, Law, Politics & Democracy (ICON-SLPD)
Conference Proceedings 2025

Legal Review of Misuse of Consumer Personal Data in Electronic Transactions Based on Article 26 of the ITE Law

AmiruddinIslami MQ. Baba[1], Rudy Indrawan[2], Martahan Siburian[3]

[a]*FakultasHukum,* UniversitasPamulang, Tangsel. *E-mail:*irbaba1998@gmail.com
[b]*FakultasHukum,* UniversitasPamulang, Tangsel. *E-mail:*awani.lkah@gmail.com
[c]*FakultasHukum,* UniversitasPamulang, Tangsel. *E-mail:*martahansiburian@outlook.com

Article

Received: Des 02, 2023;
Reviewed: Jan 07, 2024;
Accepted: Feb 09, 2024;
Published: Mar 31, 2024

Abstract

The rapid advancement of information and communication technology has significantly transformed social interaction patterns, including the rise of electronic transactions in daily economic activities. However, these developments are accompanied by increasing risks, particularly the misuse and unauthorized dissemination of consumers' personal data by business actors or cybercriminals. This study aims to analyze the legal protection of personal data belonging to consumers in electronic transactions based on Article 26 of the Electronic Information and Transactions Law (EIT Law) and its harmonization with the Personal Data Protection Law (PDP Law) in Indonesia. This research applies a normative juridical approach, focusing on statutory and conceptual analyses. The results show that Article 26 of the EIT Law establishes fundamental provisions requiring consent from data owners before their data may be used. Nevertheless, the regulation is still considered insufficient and lacks detailed enforcement mechanisms. The enactment of the PDP Law provides more comprehensive protection by strengthening the rights of data subjects and imposing clearer obligations on electronic system providers regarding lawful data processing, security standards, and accountability. To ensure optimal implementation, strong regulatory supervision, effective law enforcement, business compliance, and increased digital awareness among consumers are essential in mitigating personal data breaches within electronic transaction activities.

Keywords: Personal Data Protection; Electronic Transactions; Consumer Protection; EIT Law; PDP Law

A. INTRODUCTION

Globally, information and communication technology has transformed the way people behave in society and throughout human history. Furthermore, the rapid advancement of information technology has resulted in a borderless world and profound societal transformation. The advent of computers, information, and technology marked the beginning of the contemporary modern era. Human communication is no longer limited by time and place because advances in these fields have made it relatively simpler. Current developments are inseparable from technology. (Sri Adiningsih, 2019:58) stated that Indonesia has now entered the Industrial Revolution 4.0. Everything can be controlled from anywhere with the internet and connected devices. The impact of this era is enormous when digital-based technology is used in the daily activities of the wider community, such as increasing workforce productivity, building socio-economic relations, and simplifying various things.

The rapid development of sophisticated technology has also influenced economic activities, particularly in the field of buying and selling. Advances in technology and information technology have given rise to new innovations, namely online buying and selling transactions, also known as e-commerce. E-commerce, or online transactions, are buying and selling transactions or trade conducted electronically, involving the use of the internet, without face-to-face meetings. Therefore, many consumers are turning to online shopping due to its convenience. This is also why consumers tend to prefer online buying and selling systems over in-person visits. Despite the benefits offered, online transactions also bring a number of legal issues, particularly in the area of consumer protection. For example, legal protection of consumers' personal data is important. Because the two parties never meet face-to-face, online businesses can easily obtain personal data about their consumers.

The advantages of using technology and information are not only seen in education and business, but also in other areas related to the development of science, knowledge, and other easily accessible resources. In this case, we quickly produce billions, even trillions, of information. In work life, large amounts of data can be managed correctly, quickly, effectively,

and efficiently, with errors minimized. In business, promotions and opportunities to improve public welfare are quickly implemented across local and regional boundaries and reach all levels of society, both nationally and internationally. However, advances in science and technology not only bring results but can also give rise to conflicts that impact the public, such as: information misuse, theft of personal information, the sale of personal information, fraud, and others (Situmeang, 2021).

Personal data is specific and individual information that is always updated, authentic, and confidential. Any original and accurate information related to and allowing direct or indirect identification of any individual whose use is in accordance with the requirements of statutory regulations is considered as specific individual data. However, as the internet develops, this can result in personal data piracy among internet service users. Without their knowledge or consent, their personal data is stored, shared, and even used by third parties to carry out risky or illegal activities, such as conducting illicit online transactions by impersonating another person whose personal account has been hacked by the party; this is commonly referred to as cybercrime. As a result, the personal information of internet service users is not always protected. The security of internet service users' personal data must be maintained because this information is a person's privacy and if misused, the account holder can be negatively impacted, especially if the information is used to carry out illegal activities. The need to secure personal data stems from many main factors. (1) online bullying based on gender, (2) Stopping individuals who are careless in misusing personal information. (3) Preventing any fraud; (4) Preventing possible slander; (5) The right to manage personal information (Kurniawati & Yunanto, 2022).

As is known, Indonesia has recently experienced frequent cyberattacks from cybercriminals, resulting in the leak of personal data from several platforms in Indonesia. Recently, the public has been concerned about the leak of personal data, such as mobile phone numbers and the leak of National Identity Cards (NIK) to online lending platforms (pinjol). There has been widespread misuse of personal data, including National Identity Cards (KTP) and photos, particularly for online loan borrowers who fail to make payments. In May 2021, data from several Social Security Administration Agencies (BPJS), resulting in the data of 279 million Indonesians being leaked and sold on the online forum Raid Forums by 181 accounts named "Kotz." The dataset, containing NIKs, mobile phone numbers, email addresses, addresses, and salaries, was sold for 0.15 bitcoin, equivalent to Rp84.4 million. The data also included data on deceased residents. Two days after the alleged data leak surfaced, the BPJS Kesehatan team, along with the National Security Agency (BSSN) and the security operations system team, conducted an investigation using digital forensics and data samples from the kotz account. The account posted information about the data sale on raidforum.com. BPJS Kesehatan management then prepared a letter requesting legal protection to the Criminal Investigation Unit of the Indonesian National Police (Bareskrim Polri) and a notification letter to the Ministry of Communication and Information. BPJS Kesehatan coordinated with the Coordinating Ministry for Political, Legal, and Security Affairs, which was also attended by the National Cyber and Security Agency (BSSN), the BPJS Ketenagakerjaan (Employment Social Security Agency), and the State Intelligence Agency (BIN). BPJS Kesehatan then conducted an internal investigation assisted by BSSN. This effort was accompanied by the preparation of

mitigation measures against potential data security breaches, including the implementation of biometric fingerprint and facial recognition for service and administrative processes. Furthermore, BPJS Kesehatan also took preventive measures to strengthen its information technology security system against potential data breaches. This was done by increasing system protection and resilience.

Following up on this matter, the government stated that personal data regulations are currently contained in several laws and regulations. Therefore, to increase the effectiveness of personal data protection, President Jokowi has ratified Law No. 27 of 2022 concerning Personal Data Protection. This law serves to guarantee citizens' rights to personal protection and raise public awareness, as well as guarantee recognition and respect for the importance of personal data protection. Law No. 27 of 2022 clearly stipulates that individuals, including those conducting business or e-commerce activities from home, can be categorized as personal data controllers. Therefore, they are legally responsible for the processing of personal data they carry out and comply with the provisions of the Personal Data Protection Law (UUPDP). The scope of the UUPDP applies to personal data processing carried out by individuals, corporations, public bodies, and international organizations. (Kurniawan, 2021) The provisions in Article 26 of the ITE Law are still general and do not provide detailed definitions regarding valid forms of consent or security standards that must be implemented by electronic system providers. Therefore, in its implementation, business actors have considerable flexibility in managing consumer data without strict oversight from regulators. This causes an imbalance in the legal position between business actors and consumers.

Personal data protection is one of the human rights that is part of personal self-protection. This personal self-protection is stated in Article 28G of the 1945 Constitution which states that: "Everyone has the right to protection of personal data, family, honor, dignity and property under his control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a human right. This personal self-protection or privacy is universal, in the sense that it is recognized by many countries.

Law Number 19 of 2016 concerning Electronic Information and Transactions, specifically Article 26 paragraph (1), stipulates that any use of information regarding a person's personal data through electronic media must obtain the consent of the person concerned, unless otherwise stipulated by statutory regulations. "The use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned, unless otherwise stipulated by statutory regulations," reads the statement (Kesuma et al., 2021). Personal data is part of the right to privacy that must be protected by law. In Indonesia, the right to privacy is beginning to be recognized as a legal right inherent in an individual and is included in human rights. Although normatively this protection has been stipulated in regulations, practice in the field shows that there are still many violations that are detrimental to consumers as data owners. Cases of consumer data leaks on various digital platforms have become a legal phenomenon.

Indonesia already has several regulations governing personal data protection, although they are still partial and not comprehensive, prior to the enactment of the Personal Data Protection Law (PDP Law) in 2022. Article 26 of the ITE Law serves as the initial foundation, stating that the use of personal data must be carried out with the explicit consent of the data

owner. This provision is a crucial recognition of the right to privacy in the digital world. Furthermore, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions regulates the responsibilities of digital service providers to ensure user data security. This regulation requires businesses to implement adequate security systems and protect the confidentiality of user data from unauthorized access. Furthermore, the PDP Law strengthens the regulations by providing details on the rights of data subjects, the obligations of data controllers, and stricter sanctions for violations. However, the implementation of these regulations still faces obstacles in law enforcement. Limited legal resources, low data literacy among the public, and weak digital security systems on various platforms contribute to the continued prevalence of personal data breaches. Therefore, a strengthened oversight system and a more effective legal mechanism are needed to prosecute perpetrators of data misuse.

The above description demonstrates that the rapid development of digital technology has shifted consumer transaction patterns toward e-commerce. However, this increase has not been accompanied by adequate protection of consumer personal data. Although Article 26 of the Electronic Information and Transactions Law stipulates that all processing of personal data must be based on the data owner's consent, its implementation remains far from optimal. Misuse of personal data, information leaks, and even cybercrime continue to occur frequently due to weak data security systems and minimal regulatory oversight. Furthermore, consumers are vulnerable due to a lack of legal literacy and an imbalance in their position with business actors as data controllers. Although the government has issued Law Number 27 of 2022 concerning Personal Data Protection as an effort to strengthen more comprehensive legal protection, enforcement challenges still require concrete steps in the form of increased strict sanctions, compliance monitoring, and increased legal awareness among the public. This situation indicates that personal data protection as a human right has not been optimally realized in the context of electronic transactions in Indonesia.

B. MATERIALS AND METHODS

This scientific paper is a type of normative juridical research. This research uses a statutory approach by adopting a normative juridical perspective in examining relevant theories and principles. Normative juridical research in legal science is conducted by searching for, evaluating, and examining relevant secondary facts (library materials). The data collection method used in this research is a literature study. The data analysis technique used in this research is descriptive-analytical, namely by outlining the normative content and meaning of the collected legal materials, then analyzing them systematically and critically to answer the formulated legal problem formulation. The analysis is carried out by interpreting legal norms based on dogmatic legal principles and logical and rational juridical reasoning. In this process, the researcher not only explains legal rules textually but also assesses their coherence, normative applicability, and implications in legal practice, so that it is expected to be able to produce conclusions that are argumentative, objective, and in accordance with the principles of legal science.

C. RESULT AND DISCUSSION

Electronic Transactions are legal acts carried out using computers, computer networks, and/or other electronic media. The electronic buying and selling transaction process is a buying and selling transaction carried out by one person to another person using the internet media in an unlimited time, anytime, anywhere and is carried out in a way that does not require face to face between the parties, they only rely on trust between the parties. However, this trading business activity remains legal if each party has agreed without the need for a meeting. Electronic buying and selling transactions, one of the things related to one another is the legal subject. Regarding the legal relationship between legal subjects in this transaction, it is directly related to rights and obligations. Legal subjects in electronic buying and selling transactions are sellers, buyers, banks and providers.

The main sources of law related to the management of electronic information and transactions are Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) as amended by Law No. 19 of 2016 concerning Amendments to the ITE Law, also Government Regulation No. 82 of 2012 concerning the Implementation of Electronic Systems and Transactions (Reg. 82) and its implementing regulations, Regulation of the Minister of Communication and Information Technology No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. It should be noted that Law of the Republic of Indonesia Number 11 of 2008 is still in effect, even though it has undergone changes.

In substance, Government Regulation Number 82/2012 concerning the Implementation of Electronic Systems and Transactions (PSTE) which was promulgated and has been in effect since October 15, 2012. In Article 1 paragraph (2) it states that Electronic Transactions are legal acts carried out using Computers, Computer networks, and/or other electronic media. In Article 65 of Government Regulation Number 82 of 2012 it states that business actors who operate electronic transactions can be certified by the Reliability Certification Institute (Certification Competency) from within Indonesia or a foreign competency certification body. Although until now such an institution does not yet exist.

In response to legal developments related to internet buying and selling, the Indonesian Government has issued Law Number 11 of 2008 concerning Information and Electronic Transactions, considering that national development is a continuous process that must always be responsive to various dynamics occurring in society. Article 4 of Law Number 11 of 2008 stipulates that the use of information technology and electronic transactions is carried out to increase the effectiveness and efficiency of public services, as well as to provide a sense of security, justice and legal certainty for users and providers of information technology.

In Indonesia, the laws and regulations related to personal data in electronic media are contained in Article 26 of the Electronic Information and Transactions Law which regulates personal data as follows. Article 26 Paragraph (1) of the ITE Law states that: "Unless otherwise determined by laws and regulations, the use of any information via electronic media concerning a person's personal data must be carried out with the consent of the person concerned." In the section contained in Article 26 of Law Number 19 of 2016 concerning Electronic Information and Transactions, it is further explained what is meant by personal data protection in relation to the use of information technology. Related to the protection of personal data from unauthorized users, the contents of Article 26 of the Electronic Information and Transactions Law state that

users of every owner of personal data in an electronic media must obtain permission from the owner of the data concerned.

Technological advancements have brought significant changes in the use of the internet in human life, namely a shift in communication patterns from paper-based to paperless. Consequently, various transactions have also shifted, from conventional transactions to electronic transactions (e-commerce). In developed countries, everything is now online. Even buying and selling is increasingly conducted online through the internet. The advantage of online buying and selling is that we can simply sit in front of a computer, and everything is connected to the internet.

The use of electronic technology in online sales and purchase agreements has had a very positive impact, namely in the speed, ease, and sophistication of global interactions without the constraints of place and time, which are now commonplace. Face-to-face agreements (meeting in person) are no longer necessary for business actors, but face-to-face meetings through electronic media, so it can be said that electronic commerce has become a new economic driver in the technology sector, especially in Indonesia. Even in online sales and purchase transactions, digital signatures are used.

The advantages of using technology and information are not only seen in education and business, but also in other areas related to the development of science, knowledge, and other easily accessible resources. In this case, we quickly produce billions, even trillions, of information. In work life, large amounts of data can be managed correctly, quickly, effectively, and efficiently, with errors minimized. In business, promotions and opportunities to improve public welfare are quickly implemented across local and regional boundaries and reach all levels of society, both nationally and internationally. However, advances in science and technology not only bring results but can also give rise to conflicts that impact the public, such as: information misuse, theft of personal information, the sale of personal information, fraud, and others (Situmeang, 2021).

Personal data is a fundamental human right, namely the right to privacy. Recent technological advances experienced by most Indonesians have increased the importance of maintaining the confidentiality of personal data from potential data breaches or misuse by various parties. Data is a crucial factor, containing various personal information frequently used in digital platform activities. Data is typically used to obtain services on digital media that may not guarantee the security of their customers' personal data. This has the potential for misuse of personal data, which is difficult to account for. A person's personal data consists of several processes, including information collection, storage, processing, and data transfer from one industry to another. The more data collected, the more vulnerable it is to misuse. Personal data has become a very valuable asset. Personal information such as our names, addresses, phone numbers, and personal preferences is now being collected, exploited, misused, and traded by various entities, from large technology companies and financial institutions to mobile phone applications (Gunadi, Subrian, Lee, Gunawan, & Baretta, 2023).

Personal data theft has become a growing form of crime with the advancement of digital technology, where various activities can now be conducted through digital media. While data protection offers numerous benefits and advantages, the need for more stringent and accurate data protection software is becoming increasingly important. This is due to the

negative impacts of the development of e-commerce, which are perceived as detrimental to many people. Some of these impacts include fraudulent acts that cause direct financial losses, bank account hacking, personal data theft, and unauthorized access, which has caused public unrest (Nuranisa & Lukitasari, 2024).

Several cases of consumer personal data leaks are vulnerable to potential misuse of personal data in e-commerce electronic transactions, the financial technology industry sector (Financial Technology), and banking activities. Adisya's research reveals that the use of personal data in e-commerce is vulnerable to cyber attacks, so e-commerce users must take appropriate precautions to protect their personal data. The greater the threat to the data processing system, the higher the risk of a breach in the form of financial or non-financial security of e-commerce users' personal data. The level of effectiveness and suitability of the implemented security strategy will have a direct impact on the level of personal data security. Sagdiyah's research reveals that legal protection of consumer personal data in e-commerce transactions has great significance. Legal regulations provide a legal framework to protect consumers from potential data misuse, privacy violations, and security risks.

The increasing ease of payment transactions using e-commerce must also be accompanied by increased protection of consumer data to prevent misuse of consumer data by irresponsible parties. Based on the facts, the presence of the PayLater payment feature has actually opened up new opportunities for irresponsible parties to hack consumer accounts. This is evidenced by the emergence of cases of misuse of Traveloka consumer data to take out loans through Traveloka PayLater. The Traveloka PayLater case demonstrates the weak protection of consumer data by service providers (Sabiq, 2022). The data leak case that occurred on the Tokopedia platform in 2020, which compromised approximately 91 million user accounts, is a clear example of the risks faced by consumers in the e-commerce ecosystem (Mahfudin, 2024). This incident revealed the weakness of the security system implemented by the company, as well as the lack of accountability in the management of personal data. Violations such as this demonstrate the importance of strong legal protection to prevent similar incidents in the future.

In a legal context, data breaches such as these raise fundamental questions about corporate responsibility, consumer redress mechanisms, and the effectiveness of existing regulations. Globally, efforts to improve personal data protection have been undertaken through various legal frameworks. The European Union's General Data Protection Regulation (GDPR) serves as an example of a global standard that strictly regulates personal data governance, including consumers' rights to access, correct, and delete their data (Chisomo Tolani & Prof. Jyoti Pareek, 2024). In Indonesia, the enactment of Law Number 27 of 2022 concerning Personal Data Protection reflects the government's awareness of the urgency of data protection in the face of threats in the digital world. This law is a significant step in creating a comprehensive legal framework. However, the implementation and oversight of this law still face various challenges, including limited institutional capacity and a gap between regulations and technological developments (Nuranisa & Lukitasari, 2024).

Protection of personal data should receive legal protection from the government where it is related to personal data which is a basic human right of citizens. In its constitution, Indonesia recognizes the right to personal protection of its citizens as stated in Article 28 letter G, namely: "Everyone has the right to protection of themselves, their families, their honor, and

their property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a basic human right." This article clearly states that the state guarantees the rights and personal protection of its citizens.

Before the enactment of Law Number 27 of 2022, regulations regarding personal data protection were still partial and not comprehensive. One of the laws that regulates this is Law Number 11 of 2008 as amended by Law Number 19 of 2016. This law does regulate personal data protection, however, it is still incomplete and not comprehensive. In this law, for example, in Article 26 paragraph 1 it is stipulated that: "Unless otherwise determined by statutory regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned." Then in paragraph 2 it is stipulated that: "Any person whose rights as referred to in paragraph (1) are violated may file a lawsuit for losses incurred based on this law." In this law, prohibited acts concerning personal data are regulated, however, the problem is that this law does not clearly regulate the definition of personal data. Therefore, if using this law to file a lawsuit in the event of a dispute or criminal act, the plaintiff or reporter will experience difficulties in terms of proof. Due to this, a law is needed that comprehensively regulates the protection of personal data.

In Indonesia, regulations have been passed that regulate the protection of personal data of Indonesian citizens, which are stated in Law No. 27 of 2022 concerning Personal Data Protection, which states: Article 1 paragraph (1) Personal Data, defined as "Data about an individual who is identified or can be identified individually or combined with other information, either directly or indirectly through an electronic or non-electronic system" while Article 2 explains that "Personal Data Protection is the entire effort to protect personal data in the series of personal data processing in order to guarantee the constitutional rights of personal data subjects". In both articles, it has been emphasized that personal data is protected by law as a guarantee of the basic rights of citizens.

The Electronic Information and Transactions Law, hereinafter referred to as ITE, does not yet contain specific personal data protection regulations. However, this law implicitly gives rise to a new understanding regarding the protection of the existence of electronic data or information, both general and private. Protection of personal data in an electronic system includes protection from unauthorized use, protection by electronic system organizers, and protection from illegal access and interference. Regarding the protection of personal data from unauthorized use, Article 26 of Law Number 11 of 2008 concerning Electronic Information and Transactions requires that the use of any personal data in an electronic medium must obtain the consent of the owner of the data concerned. Anyone who violates this provision can be sued for the losses incurred. Article 26 of the ITE Law reads as follows: 26: "Unless otherwise stipulated by statutory regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned," while paragraph (2) explains that: "Any person whose rights as referred to in paragraph (1) are violated may file a lawsuit for losses incurred under this law." Article 26 paragraph (1) states that unless otherwise stipulated by statutory regulations, the use of any information via electronic media concerning a person's personal data must be carried out with the consent of the person concerned. Paragraph (2) then states that any person whose rights as referred to in paragraph (1) are violated may file a lawsuit for losses incurred based on this law.

The explanation of Article 26 paragraph (1) explains that in the use of information technology, protection of personal data is one part of personal rights (privacy rights). Personal rights have the following meaning:

1. Privacy rights are the right to enjoy a private life and be free from all kinds of interference.
2. Privacy rights are the right to communicate with others without being spied on.
3. Privacy rights are the right to control access to information about one's personal life and data.

The explanation of Article 26 of the ITE Law states that personal data is part of a person's personal rights, while the definition of personal data can be seen in Article 1 of the Government Regulation concerning the Implementation of Electronic Transaction Systems, namely certain individual data that is stored, maintained, and kept true and its confidentiality is protected. The Electronic Information and Transaction Law actually comprehensively contains provisions that regulate how data protection is provided to individuals, legal entities, and the government. The ITE Law expressly prohibits unlawful access to other people's data through electronic systems to obtain information by breaking through security systems. The ITE Law expressly states that wiretapping is a prohibited act unless it is carried out by a party who has the authority to do so in the context of legal efforts. Based on this ITE Law, everyone is prohibited in any way from disclosing other people's information for any purpose, even if the data is confidential and can be opened to the public.

The provisions stipulated in this article provide the right for personal data owners to maintain the confidentiality of their personal data. If their personal data has been disseminated and misused by another party, the personal data owner can file a lawsuit in court. The lawsuit in question is a civil lawsuit filed based on statutory regulations. The provisions of this article are the protection provided for a person's personal data in general, meaning that in every activity involving electronic transactions that use a person's personal data, it is mandatory to maintain and protect that personal data. With these regulations, everyone has the right to store, maintain and maintain the confidentiality of their data so that the data they own remains private. Any personal data that has been provided must be used in accordance with the consent of the person who owns it and its confidentiality must be maintained.

Based on this research analysis of the misuse of consumer personal data in electronic transactions, the development of digital technology and the increase in e-commerce activity are not in line with adequate personal data protection. Although Article 26 of the Electronic Information and Transactions Law stipulates the requirement for data owner consent for the use of personal information, this provision is still general and does not provide comprehensive technical standards or protection mechanisms. This situation has resulted in numerous personal data breaches such as identity theft, digital fraud, and data leaks on various platforms, indicating weak electronic system security and low business compliance in managing consumer data. Furthermore, the imbalance between business actors as data controllers and consumers with low legal literacy has resulted in people's privacy rights not being optimally protected. The enactment of Law Number 27 of 2022 concerning Personal Data Protection is an important step to strengthen the protection of the right to personal data as part of the human rights guaranteed

in Article 28G of the 1945 Constitution. However, the implementation of data protection still faces obstacles such as a lack of oversight, unclear sanctions, and a lack of readiness of digital security infrastructure. Therefore, efforts to strengthen regulations, increase public literacy, and enforce the law more effectively are urgent to ensure optimal protection of consumer personal data in electronic transactions.

D. CONCLUSION

Based on the above description, the author concludes that Article 26 of the Electronic Information and Transactions Law provides a legal basis for the protection of personal data by requiring the consent of the data owner before use. However, this regulation remains general and does not yet regulate detailed data protection standards, including security mechanisms, valid forms of consent, or the responsibilities of business actors as data controllers. This situation has led to a high rate of violations and misuse of consumer personal data, such as identity theft, data leaks by digital platforms, and fraud through illegal access to consumer accounts in e-commerce transactions. Furthermore, consumers' position is very weak due to limited digital literacy and the imbalance of power between them and business actors who control electronic systems. As a form of strengthening, the enactment of Law Number 27 of 2022 concerning Personal Data Protection serves as a more comprehensive legal instrument to ensure the guarantee of consumers' right to privacy as part of the human rights protected by Article 28G of the 1945 Constitution. However, the effectiveness of legal protection remains dependent on strict enforcement, increased oversight of business actors operating electronic systems, and public awareness in safeguarding their own personal data. Thus, the protection of personal data in electronic transactions in Indonesia requires synergy between clear regulations, compliant business actors, and empowered consumers to prevent misuse that harms the rights and security of personal data.

REFERENCES

Ardika, I. W. C. (2025). Tinjauanhukumterhadapperlindungan data pribadi di era digital: Kasuskebocoran data penggunalayanan e-commerce. *Indonesian Journal of Law and Justice*, *2*(3), 11-11.

Basri, H. (2020). *Perlindunganhukumterhadapkonsumendalammelakukantransaksi e-commerce ditinjaudariUndang-UndangPerlindunganKonsumenUndang-UndangNomor 8 Tahun 1999 (StudiKasusKerudungbyramana Bandung). TinjauanHukumPamulang, 2 (2), 131 .*

Dade, L. L., Waha, C. J., &Nachrawy, N. (2024). Kajianyuridistentangtindakpidanapenyebaran data pribadimelalui internet (doxing) di Indonesia. *Lex Privatum*, *13*(3).

Lutfia, D., & Kartika, F. B. (2022). ANALISIS PERLINDUNGAN HUKUM ATAS DATA PRIBADI KONSUMEN PENGGUNA APLIKASI SHOPEE DALAM LAYANAN TRANSAKSI ELEKTRONIK. *JurnalMimbarIlmuHukum (MIH)*, *1*(1), 75-84.

Lapian, R. (2024). PengaturanPenggunaanTandaTanganElektronikMenurutUu No. 19 Tahun 2016 TentangInformasi Dan TransaksiElektronik. *Lex Privatum*, *13*(1).

Maharani, R., &Prakoso, AL (2024). Perlindungan Data PribadiKonsumenOlehPenyelenggaraSistemElektronikDalamTransaksi Digital. *JurnalTinjauanHukumUSM* , *7* (1), 333-347.

Mediyanti, R. A., &Fithry, A. (2023). TINJAUAN YURIDIS TENTANG PERLINDUNGAN DATA DIRI MENURUT UU ITE PASAL 26 YANG DISALAHGUNAKAN. *Prosiding SNAPP: SosialHumaniora, Pertanian, KesehatandanTeknologi*, *2*(1), 121-126.

Pranindya, KRA (2025). PenegakanHukumterhadapPelakuPenyalahgunaanPenyebaran Data PribadiMelalui Barcode Ditinjaudari UU ITE dan UU Nomor 27 Tahun 2022 Tentang(UU PDP). *Konsensus: JurnalIlmuPertahanan, HukumdanIlmuKomunikasi* , *2* (3), 123-135.

Syafriana, Rizka. "Perlindungankonsumendalamtransaksielektronik." *De LegaLata: JurnalIlmuHukum* 1.2 (2016): 430-447.

Setyawati, D. A., Ali, D., &Rasyid, M. N. (2017). Perlindunganbagihakkonsumendantanggungjawabpelakuusahadalamperjanjiantransaksi elektronik. *Syiah Kuala Law Journal*, *1*(3), 46-64.

Yulianingsih, S., & Putra, R. K. (2024). AnalisisYuridistentangPerlindunganKonsumenpada E-Commerce di Indonesia: PendekatanYuridis-Normatif. *Hakim: JurnalIlmuHukumdanSosial*, *2*(4), 842-856.

Widiyanto, H., &Lunaraisah, L. (2024). PerlindunganHukumAtasKebocoran Data PribadiKonsumenTravelokaPaylaterOleh Perusahaan. *J-CEKI: JurnalCendekiaIlmiah*, *3*(6), 7351-7364.

Undang-UndangNomor 27 Tahun 2022 tentangPerlindungan Data Pribadi.

Undang-UndangNomor 11 Tahun 2008 tentangInformasidanTransaksiElektronik.

Undang-UndangNomor 19 Tahun 2016 tentangPerubahanatas UU No. 11 Tahun 2008 tentang ITE.

PeraturanPemerintahNomor 71 Tahun 2019 tentangPenyelenggaraanSistemdanTransaksiElektronik.