Jurnal Ilmu Hukum Prima
Vol. 8 No. 2 Oktober 2025
E-ISSN : 2614-2244
ISSN : 2088-5288

Legal Protection Of Consumer Personal Data In Electronic Transactions With Legal Certainty

Thomas Ericson Hadinata Sihite[1*], Dewi Iryani[2], Puguh Aji Hari Setiawan[3]
[1,2,3]Bung Karno University, Jakarta, Indonesia.
Thomas.sihite@gmail.com[1],iryani.dewi@yahoo.co.id[2], ubkpuguhaji@gmail.com[3]*

ABSTRACT

Online buying and selling can result in the leakage of consumer personal data, as seen in the breaches of user accounts on the Tokopedia and Shopee marketplaces. The data leaks on e-commerce platforms have left users' personal data unprotected. Law No. 19 of 2016 also does not specifically address personal data protection. The type of research used in this research is normative legal research. The results of this research, namely Regulations related to the protection of personal data according to the laws and regulations in force in Indonesia, include: Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions is a revision of Government Regulation Number 82 of 2012. In addition, it is also regulated in Government Regulation No. 44 of 2008 concerning the Provision of Compensation, Restitution, and Assistance to Victim Witnesses, in addition there is Article 1 paragraph (6) and Article 5 paragraph (1) Point A of the Law concerning the Protection of Witnesses and Victims, PERKOMINFO (Regulation of the Minister of Communication and Information) Number 20 of 2016 and Article 28 paragraph (1) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. These regulations are aimed at encouraging the public to respect personal data, which is part of the right to privacy, so that other people's personal data is not widely disseminated or traded for any reason. Legal protection of consumer personal data in electronic transactions with legal certainty is as stated in Article 19 of the Consumer Protection Law, which states that e-commerce startups are responsible for losses experienced by consumers by providing administrative compensation to consumers.

Keywords: Legal Protection, Personal Data, Legal Certainty.

INTRODUCTION

Today, it is clear that information plays a crucial role in economic, social, and political decision-making. Francis Bacon, a renowned philosopher during the transition from the Renaissance to the modern era, stated that knowledge itself is a powerful force. The term "knowledge" itself can be interpreted as a broader competency, where someone possesses more information than those around them. On the one hand, the large-scale investment and

E-ISSN : 2614-2244
ISSN : 2088-5288

application technology that can be realized with industrial information in recent decades depends on the information obtained, leading to the idea that data processing is an irreplaceable activity for industrial and technological success.

The rapid development of technology and information over the past few decades has driven changes in many aspects of life. Information technology has advanced so rapidly that it has transformed lifestyles and society's needs. The impact of technological advancements is deeply felt in various aspects of life, especially during the COVID-19 pandemic, where we cannot escape the need for technological assistance. The COVID-19 outbreak has impacted many business activities, including marketing, operations, sales, and customer communications. Customer needs and demands have also changed dramatically.

Tempo magazine reported that IdEA reported a 25% increase in e-commerce sales during the pandemic, a 78% increase compared to 2019.

As the most populous country in Southeast Asia, with a population of 262 million, with 140 million connected to the internet, approximately 28 million people (13% year-on-year growth) actively conduct online transactions. Indonesia's capacity, with approximately 49 million MSMEs (Micro, Small, and Medium Enterprises), has led the Indonesian government to aim to become the largest digital economy in Southeast Asia, confident it will absorb more than 26 million workers by 2020.

The development of information technology and the significant potential of the digital economy have also been accompanied by several negative impacts, including threats to citizens' rights to privacy and personal data. The right to privacy is one of the fundamental rights. The right to privacy, although not an absolute human right, legal protection of the right to privacy remains crucial in this digital economy era.

The widespread use of internet technology worldwide is a substantial factor contributing to the increase in data processing. There's no doubt that the internet has made the exchange of information between individuals easier and more widespread. The continued circulation of individual information through unauthorized internet facilities therefore raises concerns about unfair data processing activities between internet users and the companies that process the data.

Business actors or electronic system organizers can collect personal data from customers or potential customers offline or online, where digital data can be traded without the

E-ISSN : 2614-2244
ISSN : 2088-5288

knowledge and permission of the data owner or misused (for purposes other than providing, submitting digital personal data), it can also happen that connected personal data is hijacked, stolen (hacked) by third parties.

News about the rise of fraud using e-commerce sites is a common occurrence in Indonesia. People who are aware of this are reluctant or wary of using credit cards, which compromise their privacy and personal data. With the proliferation of e-commerce sites in Indonesia, there's a need for guaranteed privacy and personal data protection. Fraud is now thriving, exploiting social media platforms like Facebook and Instagram.

The right to personal data protection develops from the right to respect for private life, also known as the right to private life. The concept of private life relates to humans as living beings. Therefore, individuals are the primary holders of the right to personal data protection. Privacy is not explicitly stated in the 1945 Constitution. However, the right to privacy is implicitly contained in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia as follows:

"Everyone has the right to protection of themselves, their families, their honor, their dignity 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."

Currently, Indonesia has regulations related to the protection of the right to privacy, namely Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which was ratified on October 17, 2022 by President Joko Widodo. Before this law was passed, regulations on personal data protection were spread across several laws and regulations, including Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions, Law Number 39 of 1999 concerning Human Rights, Law Number 14 of 2008 concerning Public Information Disclosure, and Law Number 23 of 2006 in conjunction with Law Number 24 of 2013.

The misuse of personal data reveals system weaknesses and a lack of oversight, allowing personal data to be misused and resulting in losses for the data owner. Misuse, theft, and sale of personal data constitute violations of information technology law and can also be categorized as a violation of human rights, as personal data is a fundamental human right that must be protected.

E-ISSN : 2614-2244
ISSN : 2088-5288

The case occurred, precisely in May 2020, Tokopedia, the largest online shopping website in Indonesia, 91 million customer data was leaked due to the actions of a hacker. The personal data that was breached included the names of application users, email addresses, and telephone numbers. The remaining data that remained safe was Tokopedia user payment transaction data, namely in the form of digital finance OVO and credit cards. Although the hacker did not succeed in obtaining data related to financial transactions, the hacker, knowing the importance of personal data can be used for various online frauds, this hacker sold the data on the dark web for 70 million rupiah, equivalent to $ 5000 dollars. The experience from this case, the need for a Personal Data Protection Law to clarify regulations regarding data security or at least to provide clear security regarding people's personal data.

Furthermore, similar to the case involving Lazada, which in October 2020 was hit by a personal data breach, 1.1 million users of Lazada's online supermarket, RedMart, were reportedly hacked. RedMart is Lazada's online supermarket service, which provides basic food ingredients and other household needs. This resulted in the hackers illegally accessing personal information such as names, phone numbers, email addresses, addresses, passwords, and credit card numbers for RedMart users, which was then traded online.

Therefore, the enactment of the Personal Data Protection Law (PDP) is expected to provide a strong legal framework for the governance and protection of personal data of citizens and government officials. The implementation of this PDP Law will face numerous challenges. Minimizing risk is a shared responsibility, but the burden on the government's shoulders is much heavier. Much of the government manages personal data for public service purposes. Some individuals are forced to submit identification such as their national identification number (NIK) and family card (KK) numbers. Others are voluntary, for example, to apply for positions as civil servants.

RESEARCH METHODS

This research uses a normative juridical legal method with a statute approach and a conceptual approach. The research data sources were obtained through a literature study that includes primary legal materials in the form of the 1945 Constitution of the Republic of Indonesia, Law Number 1 of 2024 concerning the Second Amendment to Law Number

E-ISSN : 2614-2244
ISSN : 2088-5288

11 of 2008 concerning Electronic Information and Transactions, and Law of the Republic of Indonesia Number 27 of 2022 concerning Personal Data Protection.

Secondary legal materials come from books, legal journals, and previous research. Data analysis is conducted through systematic, contextual, and comparative legal interpretation to obtain an accurate legal construction.

RESULTS AND DISCUSSION

Regulations Regarding Personal Data Protection According to Laws and Regulations in Indonesia.

Modern data processing technology offers many advantages over slower, manual methods. However, these advances are not without their challenges. One such issue is the potential threat to individuals' right to privacy. Personal data can now be combined and stored without restrictions and is far more accessible than before these technological advancements. Personal data can be shared and manipulated in every sector, often without the owner's knowledge. Furthermore, governments and businesses may collect information from citizens, potentially threatening individual freedoms.

When using electronic media, we naturally need to enter personal data before it can be used. Personal data is very important information that must be kept confidential by the electronic media provider.

Considering that nowadays all personal data is recorded online, both in government and private sectors, and with increasingly sophisticated technological capabilities, any data or information about a person will be easily known by other people. This can lead to cybercrime that harms others, such as the distribution of personal data or its use for other purposes. These actions are illegal and can be sued for the resulting losses. Not only for the owners of personal data whose personal data has been leaked, but also for the organizers of electronic media who will lose their users because they have a bad image due to the leaking of users' personal data.

Personal data protection is a manifestation of the recognition of the human right to privacy and the security of personal information. As a country governed by the rule of law, Indonesia has developed a comprehensive regulatory framework to protect personal data in the digital space, encompassing various complementary laws and regulations.

E-ISSN : 2614-2244
ISSN : 2088-5288

Personal data protection in Indonesia is governed by several key regulations. Law No. 39 of 1999 affirms an individual's right to privacy, stating that personal data may not be used as the object of research without consent. Law No. 19 of 2016 concerning the Electronic Information and Transactions (ITE) stipulates that the use of personal data in electronic media must be based on the data owner's consent and provides the right to sue data owners whose rights have been violated.

Law No. 24 of 2013 concerning Population Administration requires the government to store, maintain, and protect the confidentiality of citizens' population data with strict access mechanisms. Technical implementing regulations, such as Ministerial Regulation No. 20 of 2016, regulate the rights of personal data owners, including the right to confidentiality, usage history, data destruction, and dispute resolution.

Government Regulation Number 71 of 2019 comprehensively defines personal data and requires electronic system providers to implement an integrated security system. Government Regulation Number 80 of 2019 regulates data protection in electronic commerce (PMSE), requiring business actors to store data with high security standards based on the principles of honest data collection, data accuracy, and limitations on the purpose of use. Financial Services Authority Regulation Number 4/POJK.05/2021 regulates data protection specifically in the non-bank financial services sector, requiring user consent for all data processing.

Based on Government Regulation No. 82 of 2012, electronic system providers are required to provide written notification to data owners following a data protection failure. The notification must contain the cause of the failure and be delivered no later than 14 days after the failure is discovered. System providers are also required to report serious violations to law enforcement or supervisory authorities.

Prior to the enactment of the PDP Law, sanctions for violations were regulated by various regulations. The ITE Law stipulates a prison sentence of six to ten years and a fine of IDR 600 million to IDR 5 billion for unauthorized access, wiretapping, or data modification. The Banking Law provides specific sanctions of two to four years' imprisonment and a fine of IDR 4 billion to IDR 8 billion for bank officials who leak confidential information.

Law Number 27 of 2022 concerning Personal Data Protection embodies the mandate of Article 28G paragraph (1) of the 1945 Constitution. The PDP Law regulates administrative

E-ISSN : 2614-2244
ISSN : 2088-5288

sanctions in the form of written warnings, termination of data processing activities, deletion of data, and a maximum fine of 2% of annual income.

The criminal sanctions in the PDP Law are designed in a graduated manner: unauthorized acquisition or collection of personal data carries a maximum penalty of five years' imprisonment and/or a fine of IDR 5 billion; disclosure of data carries a maximum penalty of four years' imprisonment and/or a fine of IDR 4 billion; while falsification of personal data carries a maximum penalty of six years' imprisonment and/or a fine of IDR 6 billion. Additional penalties include confiscation of profits and payment of compensation.

For corporations, criminal fines can be up to ten times the fine for individuals, with additional penalties in the form of freezing of business, prohibition of certain activities, closure of business premises, revocation of permits, and even dissolution of the corporation.

Personal data misuse takes various forms: illegal data sales (in the case of online transportation), the creation of fake accounts, fraud through hacking of social media accounts, espionage (tapping official communications), and illegal transactions using cloned ATM cards. Phishing is the most widespread crime, as seen in the Tokopedia and Shopee Paylater data breaches.

Based on the perpetrator, data misuse can be carried out by: individuals with fraudulent methods, companies that sell consumer data, or hackers who break into security systems on a massive scale (such as the case of the breach of 2.3 million KPU data in May 2020).

Data privacy issues in Indonesia have not yet become a major public concern. The practice of selling student databases to promote private universities occurs repeatedly without adequate law enforcement, unlike conditions in developed countries where personal identity is strictly protected.

Article 30 paragraph (1) of the ITE Law in conjunction with Article 46 paragraph (1) threatens a maximum prison sentence of six years and/or a minimum fine of IDR 600 million for illegal access to electronic systems. Article 35 in conjunction with Article 51 provides a heavier sanction, namely a maximum prison sentence of twelve years and/or a maximum fine of IDR 12 billion for manipulation of electronic information that causes losses.

E-ISSN : 2614-2244
ISSN : 2088-5288

Regulations require that personal data be stored in encrypted form after verification of its accuracy, with a minimum retention period of five years or as determined by the sector supervisory agency.

Personal data protection in Indonesia has evolved from scattered regulations to a comprehensive system through the Personal Data Protection Law (PDP). The regulatory framework reflects the state's recognition of data protection as a constitutionally guaranteed human right. However, effective protection depends on the alignment of regulations, law enforcement, public awareness, and the implementation of security standards by electronic system providers.

Legal Protection of Consumer Personal Data in Electronic Transactions with Legal Certainty

The misuse of personal data has become a serious problem, demonstrating system weaknesses and a lack of oversight. This results in losses for data owners, as seen in the leak of personal data of Tokopedia and Shopee Paylater users, which allegedly used similar hacking methods. The misuse of personal data is not only a violation of information technology laws but also a violation of human rights, as personal data is a fundamental right that must be protected.

Misuse of personal data fulfills the elements of crimes such as theft and fraud, both objectively and subjectively. Unfortunately, existing administrative, civil, and criminal sanctions are inadequate to address this crime, which is essentially a form of perfect crime. Personal data protection regulations are essential to safeguard consumer interests and provide economic benefits for Indonesia. In the digital age, where personal data holds significant value for businesses, consumers face concerns about their data being sold or used without consent. This regulation also puts Indonesia on par with developed economies that have implemented personal data protection laws.

The ITE Law was initially enacted to ensure the smooth running of e-commerce transactions and to guarantee the protection of consumer rights. The ITE Law's philosophy is to maintain the clean, healthy, and ethical use of Indonesia's digital technology for productive use. Article 4 of the ITE Law outlines the use of information technology to enhance the nation's intelligence, improve public welfare, enhance the effectiveness of

E-ISSN : 2614-2244
ISSN : 2088-5288

public services, and open up broad opportunities for citizens to advance their thinking in the field of information technology.

Prior to the enactment of the Personal Data Protection Law, data protection was regulated by various sectoral regulations. Preventive legal protection was provided through Government Regulation 82/2012, which requires electronic system providers to register their companies and certify their eligibility, and Ministerial Regulation 20/2016, which requires providers to have internal personal data protection regulations. Repressive legal protection is regulated under Article 30 of the ITE Law, which emphasizes sanctions for hackers.

After various sectoral regulations, the Personal Data Protection Law (PDP) was finally enacted to harmonize personal data regulations within a single legal framework. The PDP Law has more specific provisions than previous sectoral regulations and provides legal certainty, establishing boundaries for both the public and personal data managers. According to Sudikno Mertukusumo, legal certainty guarantees proper enforcement of the law and its legal aspects, ensuring it functions as a rule that must be obeyed.

However, following the enactment of the Personal Data Protection Law, numerous obstacles remain. First, the immediate issuance of implementing regulations is crucial, as without these implementing regulations, the PDP Law will be less effective. Second, the limited duties, functions, and authority of the Data Protection Supervisory Agency, which lacks the authority to resolve disputes through non-litigation adjudication mechanisms and the authority to issue mediation decisions regarding compensation. Third, the rigid 3x24-hour time limit applies to all sectors, as each sector has its own unique characteristics and business models. Fourth, regulations are needed to establish a personal data protection authority. Fifth, data controllers and processors must immediately undertake internal improvements to ensure compliance with the PDP Law.

The PDP Law provides an adequate legal umbrella for the digital sector and provides legal certainty for marketplace businesses and the general public. This law provides preventative legal protection aimed at preventing violations before they occur, thereby minimizing crime in the digital world.

In the Tokopedia and Shopee Paylater data breach cases, the marketplaces have not fully fulfilled their obligations as business actors, particularly in ensuring the security of

E-ISSN : 2614-2244
ISSN : 2088-5288

personal data. Their seemingly hands-off attitude fails to uphold the principles of good faith and proper consumer service as stipulated in Article 7 of the Consumer Protection Law. Both marketplaces also failed to adhere to the principles of user security stipulated in Article 2 of Law 8/1999 and the obligation to maintain data confidentiality stipulated in Article 26 of POJK 77/2016 and Articles 5 and 28 of Ministerial Regulation of the Ministry of Communication and Information Technology 20/2016. According to the regulation, every electronic system provider is required to have and develop internal regulations for personal data protection to prevent security system failures and maintain the confidentiality, accuracy, and relevance of the personal data they manage. Marketplaces should develop internal security system regulations that can protect users' personal data from various cybercrime attempts.

CONCLUSION

Regulations on personal data protection in Indonesia are regulated in several regulations, namely: Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (revised Government Regulation No. 82 of 2012), Government Regulation No. 44 of 2008 concerning Compensation and Protection of Witnesses and Victims, Law on Witness and Victim Protection (Article 1 paragraph 6 and Article 5 paragraph 1), Ministry of Communication and Information Regulation No. 20 of 2016, Law No. 1 of 2024 concerning Amendments to the ITE Law (Article 28 paragraph 1), and Law No. 27 of 2022 concerning Protection of Personal Data. These regulations aim to protect the right to privacy by preventing the unauthorized distribution and sale of personal data.

The protection of e-commerce consumers' personal data in Indonesia has been legally guaranteed through three main regulations. The Consumer Protection Law requires e-commerce startups to provide compensation for consumer losses, while Government Regulation No. 80/2019 stipulates administrative sanctions ranging from warnings to business license revocation. With the enactment of Law No. 27/2022 concerning Personal Data Protection, it is hoped that a balance will be created between consumer rights and business obligations, while also providing an effective solution to address data leaks and providing concrete protection guarantees for consumers in digital transactions.

E-ISSN : 2614-2244
ISSN : 2088-5288

BIBLIOGRAPHY

Ananthia Ayu D, Titis Anindyajati, and Abdul Ghoffar, Protection of Privacy Rights over Personal Data in the Digital Economy Era, (Jakarta: Center for Case Research and Study, and Library Management of the Registrar's Office and Secretariat General of the Constitutional Court, 2019).

Edmon Makarim, Privacy and Personal Data Protection, (Jakarta: University of Indonesia, 2019), p. 8.

European Union Agency for Fundamental Rights and Council of Europe, Supra No. 5.

Phillipus M. Hadjon, Legal Protection for the Indonesian People, (Surabaya: PT. Bina Ilmu, 1987).

Shinta Dewi Rosadi, Cyber Law: Aspects of Data Privacy According to International, Regional, and National Law, (Bandung: Refika Aditama, 2015).

Sinta Dewi, Aspects of Personal Data Protection According to International, Regional and National Law, (Bandung: Refika, 2015)

Zainal Asikin, Introduction to Indonesian Legal System, (Jakarta: Rajawali Press, 2012).

Anggraeni, SF, The Polemic of Personal Data Ownership Regulations: The Urgency for Legal Harmonization and Reform in Indonesia. Journal of Law & Development, 48(4), (2018). 814-825.

Benuf, K., Mahmudah, S., & Priyono, EA Legal Protection for Consumer Data Security in Financial Technology in Indonesia. Legal Reflections: Journal of Legal Studies, 3(2), (2019). 145-160.

J Lee Riccardi, The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?, Boston College International and Comparative Law Review, Volume 6 | Issue 1.

Lalu Aldi Bayu Damara, “Legal Protection of Consumer Personal Data from Cyber Hacking”, Scientific Journal: Faculty of Law, University of Mataram Mataram 2019.

E-ISSN : 2614-2244
ISSN : 2088-5288

Sahat Maruli Tua Situmeang,"Misuse of Personal Data as a Form of Crime Perfect in Cyber Law Perspective, "*Journal: SASI*, Volume 27 Number 1, January - March 2021:

Wiranjaya, IDGA, & Ariana, IGP Legal Protection Against Consumer Privacy Violations in Online Transactions. Kerta Semaya, 4(4). (2016). 1-5. (2021): 98-136.

Nidaul Khasanah, F., Samsiana, S., Trias Handayanto, R., Setyowati Srie Gunarti, A., Raharja, I., Raya, J., Raya Perjuangan, J., Mulya, M., Utara, B., & Barat, J. (2020). Utilization of Social Media and Ecommerce as Marketing Media in Supporting Independent Business Opportunities During the Covid 19 Pandemic. 1(1), 51–62.http://ejurnal.ubharajaya.ac.id/index.php/JSTPM, accessed on July 23, 2024 at 10:14 WIB.

IdEA: E-commerce Sales Increase by 25 Percent During the Pandemic - Bisnis Tempo.co. (nd). Retrieved December 2, 2021, fromhttps://bisnis.tempo.co/read/1404513/idea-kenaikan-penjualane-commerce-25-persen-selama-pandemi?page_num=3, accessed on July 23, 2024 at 10:14 WIB.

The birth of four Indonesian unicorns: Gojek (transportation and cross-sector), Traveloka (ticket and travel), Tokopedia, and Bukalapak (marketplace) occurred after receiving capital injections from global investors, major global retailers, or capital players who invested for resale. All four were businesses that started from the bottom and with good hard work, but depended heavily on capital to grow. The entry of large global players has made these online businesses increasingly integrated with global players who have dominated many countries. Olisias Gultom, Katrin Schneider, and Lea Mareen Preis, Digital Economy, Hopes, and Threats Learning from Indonesia, downloaded viahttp://igj.or.id/wp-content/uploads/2018/11/Industrial-Revolution-4_IGJ_AEPF12_Ind-1.pdf, accessed April 12, 2024.

See Charter of Fundamental Rights of the European Union (2012/C 326/02) Article 8.

See Jacqueline Klosek, Data Privacy in the Information Age, Greenwood Publishing United States 2000, Pp. 1 and Ulrich Sieber, The Emergence of Information Law: Object and Characteristics of a New Legal Area", Law, Information and

E-ISSN : 2614-2244
ISSN : 2088-5288

Information Technology, (Ed. Eli Ledermen/Ron Shapira), Kluwer Law International, Denhaag 2001.

Lina Miftahul Jannah, “Personal Data Protection Law and Challenges in Its Implementation”, Online Article October 3, 2022 is on the site:https://jdih.sukoharjokab.go.id/informasi/detail/89, accessed April 1, 2024.

CNBC Indonesia. (2020, May 4). Full Story of the Leak of 91 Million Tokopedia Account Data.https://www.cnbcindonesia.com/tech/20200504063854-37-155936/cerita-lengkap-bocornya-91-juta-data-akun-tokopedia, accessed on July 20, 2024 at 06.30 WIB.

Kevin Rizky Pratama, "Lazada Hacked, 1.1 Million RedMart Users' Data Hacked", is available on the website:https://tekno.kompas.com/read/2020/11/01/08095987/lazada-kebobolan-11-juta-data-pengguna-redmart-diretas, accessed July 13, 2023