Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung

Legal Protection for Consumers Over Personal Data Security in E-Commerce Transactions

Danar Widyatama[1)] & Bambang Tri Bawono[2)]
[1)] Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: danarwidyatama.std@unissula.ac.id
[2)] Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: bambangtribawono@unissula.ac.id

Abstract. *E-commerce, a technology-based trade, has transformed conventional commerce, shifting interactions between consumers and companies from direct to indirect. E-commerce has transformed the traditional business paradigm by fostering interaction models between producers and consumers in the virtual world. The trading systems used in e-commerce are designed to allow for electronic signatures. This electronic signature is designed to encompass everything from purchase to inspection and delivery. One recent case, specifically in May 2020, involved a breach of 91 million customer data on a green-colored online sales website, the largest online shop in Indonesia. Some economists argue that business is a human economic activity solely focused on profit. Therefore, any means can be used to achieve that goal. Therefore, in this section, the moral aspect cannot be used to assess business and is even considered a limitation of business activities. Online buying and selling is a new phenomenon that emerged in the context of the development of information and communication technology, where the initial goal was to prioritize efficiency of time, price, and place in its implementation. E-commerce consumers must have an account on a marketplace to make transactions by registering as a user and then filling in information including name, address, mobile phone number, email, and type of payment transaction. This data includes personal data and its security is very important. Article 1 of Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions states, "Personal Data is certain personal data that is stored, stored, and protected for its accuracy and confidentiality."*

Keywords: *Consumers; E-Commerce Transactions; Legal Protection; Personal Data Security.*

ISSN : 2830-4624

1. Introduction

E-commerce, a technology-based trade, has transformed conventional commerce, shifting interactions between consumers and companies from direct to indirect. E-commerce has transformed the traditional business paradigm by fostering interaction models between producers and consumers in the virtual world. The trading systems used in e-commerce are designed to allow for electronic signatures. This electronic signature is designed to encompass everything from purchase to inspection and delivery.[1] One recent case, specifically in May 2020, involved a breach of 91 million customer data on a green-colored online sales website, the largest online shop in Indonesia. The personal data compromised included names of app users, email addresses, and phone numbers, with the remaining data remaining secure in the form of Tokopedia user payment transaction data, including OVO digital finance and credit cards. Although the hacker failed to obtain any financial transaction data, he recognized the importance of personal data for various online frauds. He sold the data on the dark web for 70 million rupiah, equivalent to $5,000. The experience gained from this case led to the creation of the Personal Data Protection Act to clarify regulations regarding data security, or at least to ensure clear security regarding people's personal data.[2]

Some economists argue that business is a human economic activity solely focused on profit. Therefore, any means can be used to achieve that goal. Therefore, in this section, the moral aspect cannot be used to assess business and is even considered a limitation of business activities. Online buying and selling is a new phenomenon that emerged in the context of the development of information and communication technology, where the initial goal was to prioritize efficiency of time, price, and place in its implementation. It is hoped that it can improve traditional/conventional buying and selling methods, creating a new face for buying and selling transactions with fast, easy, and convenient services. In practice, online buying and selling transactions no longer bring together sellers (business actors) and consumers (buyers). These transactions occur through websites or sites, correspondence via email or other social media, and payments can also be made via the internet, mobile banking or interbank transfers, as well as through provided minimarkets. In principle, the use of information and communication technology in online buying and selling transactions is almost similar to the conventional buying and selling contract model carried out by the Indonesian people, both buying and selling contracts carried out based on the Civil Code system (hereinafter abbreviated as KUHPer) and according to the customary law system.[3]

[1]Abdul Halim Barkatullah & Teguh Prasetyo, (2005), *Bisnis E-Commerce*: Studi Sistem Keamanan dan Hukum di Indonesia, Yogyakarta: Pustaka Pelajar, p. 7.

In Indonesia, Law Number 8 of 1999 concerning Consumer Protection (UUPK) outlines the principles of business conduct. This law essentially aims to create a balance between sellers and consumers and provide consumer protection.[4]

According to Article 1 paragraph (2) of Law Number 27 of 2022 concerning Protection of Personal Data Protection explains that personal data is the whole effort to protect personal data in the series of personal data processing to guarantee the constitutional rights of personal data subjects, with the existence of the Data Protection Law, efforts must be made to increase awareness, knowledge, concern, ability and independence of consumers to protect themselves and develop the attitudes of responsible business actors, Law Number 27 of 2022 concerning Protection of Personal Data which is based on justice, balance, security and safety of consumers, as well as legal certainty, must also be able to realize a balance in protecting the interests of consumers and business actors, so that a healthy economy can be created.[5]

E-commerce consumers must have an account on a marketplace to make transactions by registering as a user and then filling in information including name, address, mobile phone number, email, and type of payment transaction. This data includes personal data and its security is very important. Article 1 of Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions states, "Personal Data is certain personal data that is stored, stored, and protected for its accuracy and confidentiality." As an electronic system organizer in a marketplace, it is obligated to meet personal data protection standards. Personal data protection is crucial in conducting online transactions because it is related to user security. Because of the vulnerable position of users, they must be protected by law.[6]

2. Research Methods

The method used in this thesis is the normative juridical research method. The normative juridical approach is an approach carried out by examining theories,

[2]Parida Angriani, Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E Commerce : Perspektif Hukum Islam dan Hukum Positif, *Jurnal Syariah Hukum*, Vol 19, No 2, 2021, p. 151.
[3]Abdul Halim Barkatullah, (2017), *Hukum Transaksi Elektronik*, Bandung: Nusa Media, p. 41.
[4]Nuhalis, "Perlindungan Konsumen Dalam Perspektif Hukum Islam Dan Undang-Undang Nomor 8 Tahun 1999", *Jurnal Ius*, Vol 3. No. 9, 2015, p. 527.
[5]Moh Issamsudin, "Efektifitas Perlindungan Konsumen Di Era Otonomi Daerah", *Jurnal Hukum Khaira Ummah,* Vol. 13. No. 1, 2018, p. 289
[6]Celina Tri Siwi Kristiyanti, *Hukum Perlindungan Konsumen*, Jakarta : Sinar Grafika, 2011, p.13.

concepts, and legal principles along with their regulations in laws relevant to this research.[7]

3. Results and Discussion

3.1. Legal Responsibility of Service Providers for Leaks of Consumer Personal Data in E-Commerce Transactions

Personal data leaks not only pose individual risks such as fraud, identity theft, and financial crime, but also impact public trust in the digital ecosystem. Consumers become more cautious, even reluctant to use certain e-commerce services due to concerns about the security of their data. 5 On the other hand, for platform providers, these leaks can damage business reputations, undermine investor confidence, and even lead to legal sanctions. Therefore, protecting personal data should not only be viewed as a moral obligation, but also as a legal responsibility inherent in every data manager, especially e-commerce platforms.

To address these challenges, the Indonesian government has enacted Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law is a crucial regulation that specifically regulates the rights of data subjects, the obligations of data controllers and processors, and sanctions for violations related to personal data protection.[8]In the context of e-commerce platforms, the Personal Data Protection Law provides a clear legal basis for enforcing legal liability for data breaches. Platforms can no longer hide behind technical claims but must instead demonstrate that they have met the principles of security, prudence, and accountability in managing users' personal data.

As a form of innovation, information technology is now capable of collecting, storing, sharing, and analyzing data. These activities have resulted in various sectors of life utilizing information technology systems, such as the implementation of electronic commerce (e-commerce) in the trade/business sector, electronic education (e-education) in education, electronic health (e-health) in health, electronic government (e-government) in government, search engines, social networks, smartphones and mobile internet, and the development of the cloud computing industry.

The importance of personal data protection has grown with the rise in mobile phone and internet users. A number of emerging cases, particularly those

[7]Munir Fuady, (2018), *Metode Riset Hukum Pendekatan Teori dan Konsep,* Depok : PT. RajaGrafindo Persada, p. 1.

[8]Siti Yuniarti, Perlindungan Hukum Data Pribadi Di Indonesia, *Jurnal Becoss*, Vol.1, 2019, p. 151

involving personal data leaks and resulting fraud or pornography, have reinforced the need for legal regulations to protect personal data.

Personal data protection is closely linked to the concept of privacy, which is the idea of preserving personal integrity and dignity.[9]The right to privacy is also the ability of individuals to determine who holds information about them and how that information is used.[10]

The right to privacy through data protection is a key element of individual freedom and dignity. Data protection is a driving force for the realization of political, spiritual, religious, and even sexual freedom. The rights to self-determination, freedom of expression, and privacy are essential to our being human.

The collection and dissemination of personal data is a violation of privacy.[11]a person because the right to privacy includes the right to determine whether or not to provide personal data.[12]Personal data is an asset or commodity with high economic value. Furthermore, there is a correlative relationship between the level of trust and the protection of certain personal data. Unfortunately, the protection of personal data is not currently regulated by a separate law but is scattered throughout various regulations. For example, Law Number 36 of 2009 concerning Health regulates the confidentiality of patients' personal conditions, and Law Number 10 of 1998 concerning Banking regulates personal data regarding depositors and their savings.

The potential for privacy violations over personal data exists not only in online activities but also in offline ones. Potential online privacy violations of personal data occur, for example, in mass data collection (digital dossiers), direct marketing, social media, the implementation of e-KTP programs, e-health programs, and cloud computing activities. The potential for privacy violations in these various activities will be discussed one by one.

*Digital dossier*which is the collection of a person's personal data in large quantities using digital technology has been started since 1970 by governments, especially in European countries and the United States.[13]Today, private companies are also engaging in digital dossiers, utilizing internet technology. These private sector

[9]Wahyudi Djafar & Asep Komarudin, (2014), *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci*, Jakarta : Elsam, p. 2

[10]Lord Ester & D, (2021), *e-commerce*, oxford university, p. 6.

[11]Edmon Makarim, (2003), *Kompilasi Hukum Telematika*, Jakarta : PT. Raja Grafindo Perkasa, p. 3.

[12]Human Rights Committee General Comment No. 16 (1988),

[13]Daniel J. Solove, (2004), The *Digital Person, Technology and Privacy in the Information Age*, West Group Publication, New York : New York University Press, p. 13-17

ISSN : 2830-4624

digital dossiers have the potential to violate individuals' right to privacy over their personal data.

In addition to digital dossiers, there's also the practice of direct selling, where sellers market their products directly. With the development of this marketing method, a database industry dedicated to collecting consumer information has emerged. Currently, there are over 550 data collection companies, now known as databases, that trade consumer information. Companies conducting transactions online obtain consumer information by purchasing it from these data collection companies.

The transaction value of consumer personal data sales in 2016 globally reached 3 billion US dollars.[14]The rapid growth of the database industry has resulted in the birth of database companies that have become globally significant revenue generators. As a result, customers' personal information has become a highly valuable asset for these companies.[15]As a result, various methods are used to collect as much personal data as possible in ways that often do not respect a person's right to privacy.

Direct marketing practices in Indonesia are widespread, particularly in the financial industry, particularly in credit card management. In practice, consumers' personal information has been traded through agents without prior permission from the information owner.[16]A common case in Indonesia is the buying and selling of consumer data. Consumers whose data is successfully obtained become marketing targets for products from companies or individuals. Many internet users also offer services to buy and sell accounts or followers. However, this practice opens up opportunities for misuse of a person's data to commit crimes. The most recent case involved fraud and embezzlement of a customer's credit card, involving suspect Imam Zahali (IZ), who caused the bank approximately Rp 250 million in losses after using the customer's credit card for cash withdrawal transactions. The proceeds were then used for personal gain, including the Hajj pilgrimage to the Holy Land of Mecca. The perpetrator obtained customer data by purchasing it online for Rp 800,000 for 25 pieces of data. Using this data, the perpetrator then contacted the victim, posing as a credit card salesperson, and offered to increase the card's credit limit.[17]

[14]Marcy E.Peek, Information Privacy and Corporate Power: Toward a Re- Imagination of Information Privacy Law, *Seton Hall Law Review*, Vol 37, 2006, p. 6-7.
[15]Tal Z. Zarsky,Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall solutions to the Problems of Information Privacy in the Internet Society, *University Miami Law Review*, Vol 58, 2004, p. 991.
[16]http://rahard.worldpress.com/2009, accessed on May 5, 2024.
[17]*Ibid*

This case demonstrates the importance of providing personal data protection on par with other countries. This would further promote and strengthen Indonesia's position as a trusted business hub, a key strategy for the Indonesian national economy.

Many crimes exploit personal data in this digital age, so it must be protected. However, many people are unaware that personal information can be misused by irresponsible third parties. In Indonesia, poor data protection has resulted in widespread hacking and data leaks. These legal incidents constitute a form of cybercrime, similar to social media hacking and hacking, leading to personal data breaches, extortion, and online fraud. It's important to note that transactions arise from a legally protected legal relationship, whether intentional or unintentional.[18]

The government is slowly recognizing the importance of regulations on personal data protection, leading to the development and drafting of legislation. While the government already has a number of personal data protection regulations, these laws remain general in nature. Number 7 of 1992 concerning Banking as amended by Law Number 10 of 1998, Law Number 23 of 2006 concerning Population Administration as amended by Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, Law Number 36 of 2009 concerning Health, Law Number 39 of 1999 concerning Human Rights, Law Number 43 of 2009 concerning Archives, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems which has been in effect since December 2016, Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems, Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions, Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems, and finally Circular Letter of the Financial Services Authority Number 14/SEOJK.07/2014 concerning Confidentiality and Security of Consumer Personal Data and/or Information.

According to the Great Dictionary of the Indonesian Language, personal data is data relating to a person's characteristics, name, age, gender, education, occupation, address, and family status. Another definition of personal data is data in the form of an identity, code, symbol, letter, or number that identifies a person's personal information, which is private and confidential. From the definition above, it is known that personal data is closely related to the security of a person's personal data. If traced to legal regulations in Indonesia, regulations regarding the

[18]Gunawan.Widjaja & Kartini Muljadi, (2003), *Pedoman Menangani Perkara Kepailitan*, Jakarta: PT Rajagrafindo, p. 111.

ISSN : 2830-4624

protection of personal data are currently regulated and guarantee legal certainty for Indonesian citizens with the enactment of Law Number 27 of 2022 concerning the Protection of Personal Data.[19]

Advances in technology and information can backfire on users, this is due to the large number of cases of misuse of personal data from users in e-commerce services, without the knowledge of the owner (user of e-commerce services).[20]There have been numerous hacking cases in Indonesia in particular, such as those reported by finance.detik.com, including a data leak at Lazada, where personal data was sold on the dark web for US$1,500. Furthermore, a data leak at Cermati e-commerce site revealed that 2.9 million users' data, including membership cards, insurance, and credit cards, were being widely traded. A recent high-profile data leak at Tokopedia e-commerce site also involved data leaks, affecting not just 1-2 million users, but tens of millions of data. This hacking incident occurred in March 2020 and affected 15 million users. Tokopedia responded to the data breach, stating that despite attempts to steal user data, such as passwords, it was still protected. Tokopedia advises all users to regularly change their account passwords for security and transaction convenience.[21]

Based on the findings and cases above, the government must be present and ready to fight against hackers who try to hack the data and information of every user on e-commerce platforms in Indonesia. There are many ways that the state and government can take, one of which is the ratification of Law Number 27 of 2027 concerning Personal Data Protection. This is motivated by the increasing and widespread incidents of data hacking and personal data leaks on e-commerce platforms, resulting in the sale and misuse of personal data by hackers.

Danrivanto Budhijanto, explains that personal rights as human rights are protection of individual rights or private rights that will increase human values, improve the relationship between individuals and their society, increase independence or autonomy to manage and obtain appropriateness, and increase tolerance and make it far from acts of discrimination and limit government power.[22]

In the economic aspect, special personal data protection will be able to strengthen Indonesia's position as a trusted business and investment center and create a conducive environment for the growth of trusted investment management and

[19]Rosalinda.Elsina Latumahina, Aspek.Hukum Perlindungan Data.Pribadi di Dunia Maya, Jurnal. GEMA AKTUALITA, *Jurnal Ilmu hukum*, Vol. 3 No. 2, December 2014, p. 16.

[20]Celina Tri Siwi Kristiyanti, (2011), *Hukum Perlindungan Konsumen*, Sinar Grafika,: Jakarta, p.13.

[21] https://finance.detik.com/berita-ekonomi-bisnis/d-5659373/kompilasi-kasus-kebocoran-data-yang-heboh-terjadi-di-indonesia/2 (accessed on May 11, 2024).

[22]Pratama Yoga Geistiar, "Perlindungan Hukum Terhadap data Pribadi.Pengguna Jasa Transportasi Online dari. tindakan penyalahgunaan oleh Pihak Ketiga, *Jurnal Garuda* Vol. 3. Nomor 1, p.10-12.

ISSN : 2830-4624

can create a good environment for the growth of global data management in the data processing industry such as cloud computing to develop in Indonesia. The rules regarding personal data protection in Indonesia are currently regulated in various laws, namely Law Number 27 of 2022 concerning Personal Data Protection, Law Number 7 of 1992 concerning Banking as Amended by Law Number 10 of 1998 concerning Banking, Law Number 36 of 1999 concerning Telecommunications, Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 7 of 1971 concerning Basic Provisions on Archiving, Law Number 8 of 1997 concerning Company Documents, Law Number 36 of 2009 concerning Health, and Law Number 23 of 2006 concerning Population Administration.

Personal data protection is a human right, part of the right to privacy, guaranteed by international legal instruments and national constitutions. Law enforcement regarding personal data protection is an effort to ensure that everyone's right to data privacy is protected. This effort is carried out by various parties, including the government, the private sector, and the public. In this regard, the government has issued regulations regarding criminal sanctions for violations of personal data protection. Provisions regarding criminal sanctions for violations of personal data protection are regulated in Article 67 of Law Number 27 of 2022 concerning Personal Data Protection, which explains the following:

1. Every person is prohibited from unlawfully obtaining or collecting personal data that does not belong to him/her with the intention of benefiting himself/herself or another person which could be detrimental to the personal data subject as referred to in Article 65 paragraph (1) shall be punished with imprisonment of up to 5 (five) years and/or a fine of up to IDR 5,000,000,000.00 (five billion rupiah).

2. Every person is prohibited from unlawfully disclosing personal data that does not belong to him/her as referred to in Article 65 paragraph (2) and shall be punished with imprisonment for a maximum of 4 (four) years and/or a maximum fine of IDR 4,000,000,000.00 (four billion rupiah).

3. "Any person who is prohibited from unlawfully using personal data that does not belong to him/her as referred to in Article 65 paragraph (3) shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah)."

ISSN : 2830-4624

3.2. Legal Protection for Consumers regarding Personal Data Security in E-Commerce Transactions.

In today's era, almost every activity is controlled by the internet. This is influenced by the rapid and rapid development of technology and information. The implications of this era are profound when digital-based technology is used by people in their daily lives, for example, to increase work productivity, build socio-economic relationships, and help simplify various things. These impacts are often felt in everyday life, such as simplifying and streamlining the flow of giving and receiving information, increasing work efficiency and effectiveness, opening up opportunities for fully online learning, and enabling interaction with others from a distance. The sophistication of these technological advances and developments has given rise to rapid changes in the business and digital worlds, for example, the emergence of applications or online service providers engaged in online commerce (e-commerce).[23]

The growth of online shopping proves that technology has a positive impact, especially in the economic and business sectors. Business actors, as parties providing e-commerce media services, should play a role in protecting the rights of their users. User rights are a business actor's responsibility to ensure the smooth running of the service, so that users feel safe and comfortable in using the application, and to take further action to prevent problems that occur because they can be detrimental to both parties: producers (sellers of goods/services) and users of online shopping media or e-commerce.

The Preamble to the 1945 Constitution, paragraph 4, states that the government has a constitutional obligation to protect the entire nation and all of Indonesia's territory, advance public welfare, educate the nation, and participate in implementing world order based on freedom, eternal peace, and social justice. In line with technological and information developments in the current digital era, the state's objectives are realized in the form of personal data protection for every citizen. Personal data protection is a constitutional right that must be fulfilled by the government through a hierarchy of laws and regulations derived from statutory regulations. The laws and regulations in Indonesia related to the protection of the public over their personal data include (1) the ITE Law and its amendments, (2) PP 71/2019 concerning the Implementation of Electronic Systems and Transactions, (3) Government Regulation Number 80 of 2019 concerning Trade Through Electronic Systems (4) Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems. Of the four provisions of these

[23]Sudikno Mertokusumo, (2009), *Penemuan Hukum*, Bandung : Citra Aditya Bakti, p. 38.

laws and regulations, none specifically regulates the protection of the public's personal data related to its use in electronic systems.

The ITE Law regulates the protection of personal data and privacy rights as stated in Article 25 and 26 paragraph (1) of the ITE Law, namely:

Article 25

Electronic Information and/or Electronic Documents compiled into intellectual works, internet sites and intellectual works contained therein are protected as Intellectual Property Rights based on the provisions of Statutory Regulations.

Article 26

1. 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.

2. Any person whose rights as referred to in paragraph (1) are violated may file a lawsuit for losses incurred based on this Law.

The ITE Law also regulates the responsibilities of electronic system organizers, which are regulated in Article 15, namely:

(1) Every Electronic System Organizer must organize the Electronic System reliably and safely and be responsible for the proper operation of the Electronic System.

(2) Electronic System Organizers are responsible for the implementation of their Electronic Systems.

(3) The provisions as referred to in paragraph (2) do not apply if it can be proven that there was a force majeure, error and/or negligence on the part of the user of the Electronic System.

The explanation of Article 26 paragraph (1) of the ITE Law states that personal rights in the article contain several meanings, namely (1) rights are the right to enjoy a private life and be free from all kinds of interference, (2) personal rights are the right to be able to communicate with others without being spied on, and (3) Personal rights are the right to monitor access to information about a person's personal life and data. Thus, as determined by Article 26 paragraphs (1) - (2) of the ITE Law, the use of any information and personal data through electronic media carried out without the consent of the data owner is a violation. Although there is recognition of the protection of the right to privacy over personal data in

electronic information and transactions in Article 26 paragraphs (1) - (2) of the ITE Law. Article 26 paragraph (1) of the ITE Law clearly mandates electronic system organizers to provide efforts to protect personal data. In the use of any information related to a person's personal data, it must be carried out by the person concerned, namely the owner of the personal data. Regarding who must protect personal data, this is stated in Article 15 paragraph (1) of the ITE Law, which states "Every Electronic System Organizer must organize the Electronic System reliably and safely and be responsible for the proper operation of the Electronic System." Therefore, personal data must be protected reliably and safely to prevent failure of personal data protection in e-commerce media.[24]

The definition of personal data is not found in the ITE Law, but is explained in Article 1 number 29 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, hereinafter referred to as PP PSTE. In Article 1 number 29 of PP PSTE it is stated that what is meant by personal data is "any data about a person whether identified and/or identifiable individually or combined with other information either directly or indirectly through Electronic and/or non-electronic Systems". Based on Article 3 paragraph (1) it is mandated that electronic system organizers must organize electronic systems that are reliable and safe in the operation of electronic systems. This is also emphasized in the provisions of Article 31 of PP PSTE where Electronic System organizers are obliged to protect their users and the wider community from losses caused by the Electronic Systems they organize.

Protection of personal data is also regulated in Government Regulation Number 80 of 2019 concerning Trade Through Electronic Systems, hereinafter referred to as the PMSE PP. The PMSE PP also regulates the protection of personal data in the context of trade through electronic systems as stated in Article 58 - Article 59 of the PMSE PP. Based on Article 58 paragraph (1) of the PMSE PP that "every personal data is treated as the personal property of the person or Business Actor concerned" and Article 58 paragraph (2) of the PMSE PP that "Every Business Actor who obtains personal data as referred to in paragraph (1) is obliged to act as a trustee in storing and controlling personal data in accordance with the provisions of laws and regulations". In the provisions of Article 58 - 59 of the PMSE PP only regulates the mandate for business actors to manage personal data belonging to the public without any regulations regarding sanctions or responsibilities in the event of failure to protect personal data. In addition, personal data protection is also regulated in the Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems, hereinafter referred to as PERMENKOMINFO 20/2016. The personal data referred to is data owned by an individual or certain person

[24]Chandra Adi Gunawan Putra, "Perlindungan Hukum Terhadap Konsumen dalam Persfektif Kesadaran Hukum Masyarakat", *Jurnal Analogi Hukum*, Vol.5, No.1, 2023.

which must be stored, maintained, and kept accurate and protected. The scope of personal data protection includes "data acquisition, data collection, data processing, data analysis, data storage, display, announcement, delivery, dissemination, and destruction of personal data".

There are two types of personal data regulated by the Personal Data Protection Act: specific personal data and general personal data. The classification of this data distribution is as follows:

(1) Personal Data consists of:

a. Personal Data of a specific nature.

b. General Personal Data;

(2) Specific Personal Data as referred to in paragraph (1) letter a is as follows:

a) health data and information;

b) biometric data;

c) genetic data;

d) criminal record;

e) child data;

f) personal financial data; and/or

g) other data in accordance with statutory provisions.

(3) General Personal Data as referred to in paragraph (I) letter b includes:

a) full name;

b) gender;

c) citizenship;

d) religion; and/or

e) Marital Status/ and or;

f) Personal Data combined to identify an individual.

ISSN : 2830-4624

Efforts to regulate the right to privacy over personal data are a manifestation of the recognition and protection of basic human rights. The existence of the Personal Data Protection Law has realized the legal ideal of protecting society both normatively and constitutionally. By providing protection for these personal rights, it also means providing protection for the right to freedom of speech, which guarantees protection from the threat of fear for doing or not doing something that is a fundamental right. This concept of personal data protection emphasizes that everyone has the right to decide when to share data with others or to share data with others and determines the conditions that must be met during the data sharing process within a community.

The use of the internet in various aspects of life has not only made things easier, but has also given rise to a number of problems, including legal issues. One such legal issue is the issue of personal data protection (the protection of privacy rights). The threat of personal data misuse in Indonesia has become increasingly prominent, especially since the government launched the electronic ID card (e-KTP) program, a government-mandated personal data recording program. The e-KTP program was first launched in early 2011, implementing the National Identification Number (NIK) program. This program requires a single, lifelong identity card for each resident, containing the NIK. Furthermore, the government records population data as part of this program. All personal information of citizens is recorded, including their identities and physical characteristics. Specifically, physical characteristics are recorded by scanning fingerprints and retinas, which will be used for biometric validation of KTP holders. According to the Ministry of Home Affairs, the recorded data will then be embedded in the KTP, after first being encrypted using a specific cryptographic algorithm. Personal data recorded in e-KTP is vulnerable to misuse by irresponsible parties, especially if security is lacking.[25]

Rapid technological developments have made it easier for businesses to sell goods and services digitally through the internet, one of which is online shops. Due to the ease of conducting online transactions, many people are turning to e-commerce. Through e-commerce, business activities can be carried out anywhere and anytime. This certainly has a positive impact on offline stores that try to market their products online, thus forming a group of sellers through the marketplace and becoming part of e-commerce. E-commerce, or in Indonesian, electronic commerce, is the activity of distributing, selling, buying, marketing products (goods and services) by utilizing telecommunications networks such as the internet, television, or other computer networks. One example of an e-

[25]Sri Endah Wahyuningsih, Tinjauan Yuridis Peranan Lembaga Perlindungan Saksi dan Korban (LPSK) Dalam Melindungi Saksi Tindak Pidana Korupsi, *Jurnal Ilmiah Sultan Agung*, Vol. 6. No. 1, 2023.

ISSN : 2830-4624

commerce market platform in Indonesia is Shopee, Bukalapak, Blibli, Tokopedia, and many more.[26]

*E-Commerce*It involves more than one company and can be applied to almost any type of business relationship. Based on its scope, it can be classified as follows:

1. Internet Commerce;

2. Trading with Internet Web facilities (Web commerce);

3. Trading with Electronic Data Interchange Systems.

Meanwhile, in conducting payment transactions, consumers' identity and personal data are required to complete the transaction. In shopping activities, payment methods are, indirectly or directly, one of the important factors that are attached and are often a consideration for consumers when transacting online. Lack of trust is due to fear of fraud and lack of security due to misuse of personal data when conducting online transactions.[27]

In order to provide a sense of security and public trust regarding personal data in e-commerce transactions, Law Number 27 of 2022 concerning Personal Data Protection explains several rights held by data subjects, namely:

Article 5

Personal Data Subjects have the right to obtain information about the clarity of their identity, the basis of legal interests, the purpose of the request and use of Personal Data, and the accountability of the party requesting Personal Data.

Article 6

Personal Data Subjects have the right to complete, update and/or correct errors and/or inaccuracies in Personal Data about themselves in accordance with the purposes of processing Personal Data.

[26]Sekaring Ayumeida Kusnadi, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, *"JA: Jurnal Al-Wasath",* Vol.2, No.1, April 2021.
[27]*Ibid,* p. 30

ISSN : 2830-4624

Article 7

Personal Data Subjects have the right to gain access and obtain copies of Personal Data about themselves in accordance with the provisions of laws and regulations.

Article 8

Personal Data Subjects have the right to terminate processing, delete and/or destroy Personal Data about themselves in accordance with the provisions of laws and regulations.

Article 9

The Personal Data Subject has the right to withdraw consent to the processing of Personal Data about him/her that has been given to the Personal Data Controller.

Article 10

Personal Data Subjects have the right to object to decisions based solely on automated processing, including profiling, which produce legal consequences or have a significant impact on the Personal Data Subject.

Article 11

Personal Data Subjects have the right to delay or limit the processing of Personal Data in a proportionate manner to the purposes for which the Personal Data is processed.

Article 12

Personal Data Subjects have the right to sue and receive compensation for violations of the processing of Personal Data about them in accordance with the provisions of laws and regulations.

Article 13

1) Personal Data Subjects have the right to obtain and/or use Personal Data about themselves from the Personal Data Controller in a form that conforms to the structure and/or format commonly used or can be read by electronic systems.

2) Personal Data Subjects have the right to use and send Personal Data about themselves to other Personal Data Controllers, as long as the systems used can

communicate securely with each other in accordance with the principles of Personal Data Protection under this Law.

The right to privacy is an inherent right of individuals to choose not to disclose or choose to disclose their personal data. Therefore, accessing, collecting, or disseminating personal data constitutes a privacy violation.[28]Regulations regarding personal data protection have regulated various prohibitions regarding personal data as regulated in Article 65 of Law Number 27 of 2022 concerning Personal Data Protection, namely;

4. "Everyone is prohibited from unlawfully obtaining or collecting personal data that does not belong to them with the intention of benefiting themselves or others which could be detrimental to the subject of the personal data.

5. Every person is prohibited from unlawfully disclosing personal data that does not belong to him.

6. Every person is prohibited from unlawfully using personal data that does not belong to him or her."

4. Conclusion

Legal protection of consumers' personal data in e-commerce transactions is part of citizens' constitutional rights, which must be protected by the state. The rapid development of information and communication technology has brought various conveniences to human activities, particularly in the field of electronic commerce/e-commerce. However, behind this convenience, challenges arise related to personal data security. Electronic transactions open up significant opportunities for misuse of personal data by irresponsible parties, such as hacking, identity theft, or digital fraud that harm consumers. Responding to these challenges, the state has attempted to provide consumer protection through various legal instruments. Several important regulations that have been issued include Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Law Number 27 of 2022 concerning Personal Data Protection. The legal responsibility of e-commerce providers for data breach threats has become stronger after the government passed Law Number 27 of 2022 concerning Personal Data Protection, which stipulates administrative and criminal sanctions for violations of misuse or negligence in personal data management. Digital service providers are required to

[28]Samudra Putra Indratanto, Nurainun, and Kristoforus Laga Kleden, "asas kepastian hukum Dalam implementasi putusan mahkamah konstitusi berbentuk peraturan Lembaga negara dan peraturan pemerintah pengganti undang-undang," *Jurnal Imu Hukum*, vol.16, no. 1 (2020).

implement a risk-based security system, report any breach incidents, and assume full responsibility for managing their consumer data. This obligation includes the application of the principles of prudence, accountability, and transparency at every stage of data processing, from data acquisition and storage to data destruction. With this regulation, e-commerce providers are not only required to comply with the law but also to actively create a culture of data protection as a form of respect for consumer rights in the digital age.

5. References

Journals:

Chandra Adi Gunawan Putra, "Perlindungan Hukum Terhadap Konsumen dalam Persfektif Kesadaran Hukum Masyarakat", *Jurnal Analogi Hukum*, Vol.5, No.1, 2023.

Marcy E.Peek, Information Privacy and Corporate Power: Toward a Re-Imagination of Information Privacy Law, *Seton Hall Law Review*, Vol 37, 2006

Moh Issamsudin, "Efektifitas Perlindungan Konsumen Di Era Otonomi Daerah", *Jurnal Hukum Khaira Ummah,* Vol. 13. No. 1, 2018

Nuhalis, "Perlindungan Konsumen Dalam Perspektif Hukum Islam Dan Undang-Undang Nomor 8 Tahun 1999", *Jurnal Ius*, Vol 3. No. 9, 2015

Parida Angriani, Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E Commerce : Perspektif Hukum Islam dan Hukum Positif, *Jurnal Syariah Hukum*, Vol 19, No 2, 2021

Pratama Yoga Geistiar, "Perlindungan Hukum Terhadap data Pribadi.Pengguna Jasa Transportasi Online dari. tindakan penyalahgunaan oleh Pihak Ketiga, *Jurnal Garuda* Vol. 3. Nomor 1

Rosalinda.Elsina Latumahina, Aspek.Hukum Perlindungan Data.Pribadi di Dunia Maya, Jurnal. GEMA AKTUALITA, *Jurnal Ilmu hukum*, Vol. 3 No. 2, December 2014

Samudra Putra Indratanto, Nurainun, and Kristoforus Laga Kleden, "asas kepastian hukum Dalam implementasi putusan mahkamah konstitusi berbentuk peraturan Lembaga negara dan peraturan pemerintah pengganti undang-undang," *Jurnal Imu Hukum*, vol.16, no. 1 (2020).

Sekaring Ayumeida Kusnadi, Perlindungan Hukum Data Pribadi Sebagai Hak Privasi, *"JA: Jurnal Al-Wasath",* Vol.2, No.1, April 2021.

Siti Yuniarti, Perlindungan Hukum Data Pribadi Di Indonesia, *Jurnal Becoss*, Vol.1, 2019

Sri Endah Wahyuningsih, Tinjauan Yuridis Peranan Lembaga Perlindungan Saksi dan Korban (LPSK) Dalam Melindungi Saksi Tindak Pidana Korupsi, *Jurnal Ilmiah Sultan Agung*, Vol. 6. No. 1

Tal Z. Zarsky,Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall solutions to the Problems of Information Privacy in the Internet Society, *University Miami Law Review*, Vol 58, 2004

Books:

Abdul Halim Barkatullah & Teguh Prasetyo, (2005), *Bisnis E-Commerce*: Studi Sistem Keamanan dan Hukum di Indonesia, Yogyakarta: Pustaka Pelajar

Abdul Halim Barkatullah, (2017), *Hukum Transaksi Elektronik*, Bandung: Nusa Media

Celina Tri Siwi Kristiyanti, (2011), *Hukum Perlindungan Konsumen*, Sinar Grafika,: Jakarta

Daniel J. Solove, (2004), The *Digital Person, Technology and Privacy in the Information Age*, West Group Publication, New York : New York University Press

Edmon Makarim, (2003), *Kompilasi Hukum Telematika*, Jakarta : PT. Raja Grafindo Perkasa

Gunawan.Widjaja & Kartini Muljadi, (2003), *Pedoman Menangani Perkara Kepailitan*, Jakarta: PT Rajagrafindo

Lord Ester & D, (2021), *e-commerce*, oxford university

Munir Fuady, (2018), *Metode Riset Hukum Pendekatan Teori dan Konsep,* Depok : PT. RajaGrafindo Persada

Sudikno Mertokusumo, (2009), *Penemuan Hukum*, Bandung : Citra Aditya Bakti

Wahyudi Djafar & Asep Komarudin, (2014), *Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci*, Jakarta : Elsam

Internet:

https://finance.detik.com/berita-ekonomi-bisnis/d-5659373/kompilasi-kasus-kebocoran-data-yang-heboh-terjadi-di-indonesia/2 (accessed on May 11, 2024).

http://rahard.worldpress.com/2009, accessed on May 5, 2024.

ISSN : 2830-4624

Regulation:

Human Rights Committee General Comment No. 16 (1988)