Implementation Of Legal Protection For Consumer Personal Data In E-Commerce Transactions

Yapiter Marpi

{ yapitermarpi@gmail.com}

University of Jakarta

Abstract. Economic activity has been able to rise dramatically as a result of e-commerce transactions. This study employs a normative legal research methodology that combines a conceptual and statutory approach. The findings demonstrate that a human right is the protection of private information as part of privacy. Both the constitution and a number of statutory provisions attest to this acknowledgment. However, the statutory level of private data protection is not governed by any particular rules. Regarding the use of private information in online transactions, Indonesia has no laws. Only Essay 26 of the ITE Law and a few other provisions address this matter. Economic institutions that come from internet transactions are at risk due to inadequate privacy and private data security. In order to facilitate online consumer transactions, consumers must have legal protection. Regardless of the media chosen, the goal is to complete every transaction in the same manner.

Keywords: Legal Protection; Private Data; E-Commerce.

1 Introduction

As corporate development enters the fifth industrial revolution, Indonesia is a part of it. With the help of connected devices and the internet, anything can be managed remotely. Although they are dispersed over multiple laws, Indonesia now has numerous provisions pertaining to the protection of private data. Indonesia does not yet have specific laws and regulations that regulate the legal protection of private data which could be a solution in various cases related to misuse of private data. Trade transactions can be carried out easily and quickly through e-commerce. E-commerce is the process of trading transactions, be it goods, services or information using the online internet network. The presence of e-commerce has been able to increase economic activity significantly. The concept of e-commerce with the presence of a market place has changed the concept of transactions. E-commerce has trade traffic, both locally and internationally.[1]

Law Number 27 of 2022 on the Protection of Private Data is now in effect in Indonesia. When people use digital-based technology in their daily lives, such as to improve work productivity, strengthen socioeconomic relationships, and make various tasks easier, the ramifications of this period are enormous. Information technology for computer-based communication has advanced extremely quickly in society. 40 citizen rights are among the constitutional rights outlined in the 1945 Constitution. The privilege to private protection is one among them. The

ICL-C 2023, November 11, Jakarta, Indonesia

DOI 10.4108/eai.11-11-2023.2351707

protection of individuals, their families, their honor, dignity, and property under their control is outlined in Essay 28 G, Paragraph 1 of the Constitution. Private rights are presumed to be property rights in this Essay. However, private rights should not be limited to property rights due to the advancement of information and communication technology. The privilege to privacy should be included in private rights. More delicate in nature, The privilege to privacy can stand in for individual rights.[2]

Private rights pertain to sensitive issues concerning an individual's idUnit or private information. The Population Identification Card (KTP), Driver's License (SIM), Passport, Family Card (KK), Taxpayer Identification Number (NPWP), Account Number, Fingerprints, or other private traits are the first steps in establishing this identification.[3]

At least Indonesia can compare it with the private data protection regulations that other countries have, namely Hong Kong, Malaysia, Singapore, South Korea. Some of these countries have special regulations that guarantee the legal protection of private data. However, this research will examine the comparison of Malaysia's private data protection regulations with the PDT Bill that Indonesia currently has. This comparison was made because the atmosphere of life in Malaysia is not much different from Indonesia. Even though the atmosphere of life in Indonesia and Malaysia is not much different, the legal systems between Indonesia and Malaysia have differences. The legal system in Indonesia applies a civil law legal system, namely written law (codification). There is a strict and clear separation between public law and private law.[4]

Meanwhile, the legal system in Malaysia applies a common law system, which is dominated by unwritten law or customary law through judge decisions. There is no strict and clear separation between public and private law. The universality concept, which maintains that all countries must participate in upholding the international legal system, can be utilized in light of these differences in legal systems, particularly for the benefit of global interests.

The processing of private data, including sensitive user data that could result in financial losses or even jeopardize the owner's security and safety if given to careless parties, is one of the protections of private data. Economic growth brought about by online transactions is linked to threats resulting from inadequate privacy and private data security.

2 Research Method

This study used normative legal research as its methodology. The legislative approach and the conceptual approach are the methods that are employed. Qualitative data are used in the legal texts. A conceptual approach is the method used in this study. In cases where researchers adhere to current legal regulations, they employ a conceptual approach [7] Secondary info from prestigious legal materials is what legal sources are. Legal information was gathered from Indonesian laws and rules pertaining to the protection of private information. Qualitative descriptive data analysis was employed.[8]

3 Result and Discussion

3.1 Legal Protection of Consumer Personal data in E-Commerce Transactions

The Dutch word for "consumer" is "consument." The definition of "consumer," according to legal authorities, is "the ultimate user of goods and services (Uiteindelijke Gebruiker van Goerderen en Diensten) that the entrepreneur hands over to them." (ondernamer)".[9]

"Everyone who legally obtains and uses goods or services for a particular use" is how Az. Nasution defines a consumer.

As per UUPK's Essay 1 Point (2), "Anyone who uses products and/or services that are available in society, whether for their own benefit, the benefit of their family, the benefit of others, or the benefit of other living things, and is not traded, is considered a consumer." People or companies who provide goods and/or services to meet consumer or social wants while aiming for financial benefit are generally referred to as business players. As an alternative to the term "consumer," the consumer protection law (UUPK) appears to strive to avoid using the word "producer." As a result, the phrase "business actor" is used, which has a wider definition and can refer to producers, distributors, sellers, creditors (money providers), and other terms that are frequently used.

In accordance with Essay 1 number (3) UUPK, what is by a company actor is "Any person or business organization, whether a legal or non-legal Unit, that is founded, resides, or conducts business inside the Republic of Indonesia's jurisdiction, either alone or in partnership. together using contracts to conduct business in a range of economic domains." As a result, it can be said that the definition of a business actor is as stated in Essay 1 number (3) UUPK, which describes any individual or business Unit—whether a legal or non-legal Unit—that is founded and domiciled in the Republic of Indonesia or engages in activities there, both independently and in concert through agreements to engage in business activities across a range of economic sectors. Consumers, on the other hand, are anyone who makes use of the products and/or services that are offered in society, whether for their own advantage, that of their family, that of other people, or that of other living things, and as opposed to trade.[6]

In addition to making life easier, using the internet in many ways can lead to a number of issues, including legal issues. The protection of private data is one of the legal issues that come up. Frequently, when a user registers online or completes a purchase, they are required to submit specific private information.[10]

Several legal subject areas need to be regulated in order to protect private data. The term "Private Data Manager" refers to individuals, public or private legal bodies, and other social organizations that either individually or in concert manage private data. Using data processing tools, either automatically or manually, in a structured way, and with data storage systems, private data managers perform "private data management" activities, which include but are not limited to data collection, processing, use, disclosure, dissemination, and security.[11]

Customers who use online transactions without proper safeguards are more concerned about online system vulnerabilities, especially the possibility of tampering with private information about financial or medical conditions that they regularly provide to banks, retailers, insurance agents, and credit card companies. Before initiating a transaction, consumers, as parties in

need of a product, are frequently asked to furnish full details about their private or business identities (if the customer is a firm). It is natural for producers to be able to assess consumer credibility, whether consumers are serious buyers or not. Internet site services can be accessed without having to be a member of the site, for example sites on mass media. However, there are also those that require visitors/users to register first in order to enjoy the site's services, for example electronic mail (e-mail) sites, buying and selling sites, social networking sites (social media), and others.

User registration is not only done via desktop/computer but can also be done via smartphone. To become a member, a person is generally required to fill out a kind of registration form on the site regarding private information such as name, e-mail (if any), place of residence, age, gender, occupation, etc.[12]

Data in the form of an individual's private identification, codes, symbols, letters, or numbers is referred to as private data. Germany and Sweden, which controlled the protection of private data by legislation in the 1970s, were the first countries to use the term "data protection." Because computers were then being utilized as a tool for storing population data, particularly for population census purposes, the protection was necessary. In actuality, however, both the public and private sectors have committed numerous infractions. Regulation is therefore required to ensure that private data is not exploited.

There are two ways to safeguard private information: by physically securing the information itself and by enacting laws that seek to ensure privacy in how that information is used. Private data protection regulations are currently in place in at least 107 countries.

Provisions of the Data Protection Act of 1998, which permit data subjects to request information about how their private data is processed and to stop specific data processing if it is thought to be detrimental to their interests, serve as evidence of the protection of individual privacy rights. Additionally, data should only be utilized for as long as it is required and should not be retained for longer than is necessary. This Act's protection of private data is so robust that it even forbids its transfer to non-European nations unless those nations can provide comparable data protection.[13]

The terms used to refer to private data and private information vary by nation. Nonetheless, the two phrases are frequently used interchangeably because they essentially signify the same thing. While the European Union nations and Indonesia itself use the phrase "private data" in the ITE Law, the United States, Canada, and Australia use the term "private information."

The phrase "privacy" is also used in many industrialized nations to refer to a right that needs to be upheld, namely the right of an individual to have their private life unhindered. Warren and Brandheis were the first to define the concept of privacy when they published "The privilege to Privacy" (also known as the right not to be bothered) in the Harvard University Law School scientific magazine. This journal states that Warren and Brandheis claim that as technology has advanced, people have become more conscious of the fact that everyone has The privilege to enjoy life. One definition of The privilege to live life is the freedom from interference in one's private life, whether by the government or other individuals. Thus, The privilege to privacy must be acknowledged and safeguarded by the law. It is somewhat challenging to define privacy because different people will set different boundaries for it based on their perspective.[14]

Everyone now has new rights as a result of the 2010 PDPA, including The privilege to know about their private information and the ability to access, update, and manage how their information is processed or used by third parties. The PDPA also regulates the transmission of private data across international borders. According to the PDPA, private data can only be transferred outside of Malaysia to locations chosen by the Minister of Information, Culture, and Communications. If private data is being transmitted to a destination country, the country must have a sufficient degree of protection that is at least as high as the PDPA's level.

Because Indonesia does not yet have legal tools that are responsive to the community's needs for improved protection, there is still uncertainty surrounding the protection of privacy and private data. In the age of the digital economy, legal tools for protecting private information and privacy must fulfill three requirements at the very least: (1) has an international nature; and (2) are a component that unites people and the economy. The first requirement is that cross-border agreements promote the protection of privacy and private information. These regulations include requiring specific permission for transfers of private information and privacy outside the nation's borders and limiting such transfers to nations with comparable privacy and private data protection. The second feature is the necessity of protecting private rights in addition to privacy and private data in the age of the digital economy. In other words, they must be both positive and negative rights, meaning that the state must have an active role in order for the privilege to be satisfied. Negative rights require the state to refrain from taking action.[15]

Although Law No. 8 of 1999 does not yet govern legal protection for consumers in e-commerce transactions, it does govern consumer rights and legal protection for consumers generally, and as of right now, Indonesian consumers continue to apply this law

3.2 Regulation of Consumer Personal Data in E-Commerce Transactions

The evolution of consumer rights, which are affirmed in UN resolution Number 39/248 of 1985 concerning consumer protection and are achieved in Indonesia in the UUPK, is the source of the now recognized and existing consumer rights. A number of consumer interests that must be safeguarded are also outlined in United Nations (UN) Resolution Number 39/248 of 1985 concerning Consumer Protection (Guidelines for Consumer Protection), including:[16]

1) Protection of consumers from risks to their health and safety;
2) Advancement and defense of consumers' socioeconomic interests;
3) Provision of sufficient information to allow consumers to make decisions based on their own preferences and requirements;
4) Consumer education;
5) The opportunity to establish consumer associations or other pertinent organizations and give them the chance to express their views in the decision-making process pertaining to their interests;
6) The availability of effective compensation measures.

The privilege to security (also known as the privilege to safety), The privilege to information (also known as The privilege to information), the freedom to select (also known as The privilege to choose), and The privilege to be heard (also known as The privilege to be heard)

are generally recognized as the four fundamental consumer rights. Zoemrotin K. Susilo asserts that the following consumer rights must be upheld: The privilege to safety and security; The privilege to accurate and truthful information; The privilege to select the necessary goods or services; The privilege to be heard; The privilege to compensation; and The privilege to a hygienic and healthy environment.[10]

In the meanwhile, UUPK requires the following consumer rights to be upheld:

1) The privilege to comfort, security, and safety when consuming products and/or services;
2) The privilege to select goods and/or services and acquire them in line with the terms and promised assurances, as well as the exchange rate;
3) The privilege to accurate, transparent, and truthful information about the state and guarantee of products and/or services;
4) The privilege to have voiced concerns and grievances about the products and/or services utilized;
5) The privilege to proper advocacy, protection, and efforts to settle consumer protection issues;
6) The privilege to consumer education and advice;
7) The privilege to reasonable, truthful, and nondiscriminatory treatment or service;
8) The privilege to reimbursement or replacement in the event that the goods or services are not as agreed upon or as they should be;
9) Rights governed by additional statutory requirements.

Law Number 27 of 2022 concerning Private Data Protection contains provisions governing Indonesia's current policy or regulation regarding the protection of private data. Only general features of private data protection are covered by the regulations pertaining to this topic, which are nevertheless found individually in a number of laws and regulations. The ITE Law contains several rules pertaining to the security of private information of internet users. ITE Law. Specific regulations for the protection of private data are not yet included. But the ITE Law doesn't explicitly state so. offers a fresh perspective on how to safeguard the presence of electronic data and information, both public and private. The ITE Law also requires that private electronic data be elaborated in PP PSTE.[20]

According to the ITE Law, safeguarding private information in an electronic system entails preventing illegal access and interference, as well as safeguarding it from unauthorized use and exploitation. In terms of safeguarding private information against misuse, Essay 26 of the ITE Law mandates that any use of private information in electronic media must be approved by the data's owner. Anyone who breaks this clause could be sued for their damages. According to Essay 26 of the ITE Law, private data is a component of an individual's private rights. Essay 1 PP PSTE, on the other hand, defines private data as specific individual information that is kept, preserved, and verified as accurate and secret.[15]

Although it has been broadly controlled under the ITE Law and a number of other laws and regulations, Indonesia believes that particular regulations pertaining to the protection of private data must be made right away. Improving Indonesia's economic standing in global trade is one of the primary motivations. Because business relationships involve an automatic

transfer of data, developed nations like the European Union or Singapore will no longer be hesitant to conduct business with Indonesians through cyberspace if Indonesia already has strong and sufficient regulations. Developed nations stress that only nations with equally robust privacy protections may receive data transfers.

Aside from financial considerations, human rights legislation must include stronger privacy regulations. Human rights include The privilege to privacy, and one method to uphold this right is by implementing special measures to secure private information.

There is now no law in Indonesia that expressly and explicitly governs the protection of private data and privacy, which raises concerns. As a result, in the current period, privacy and the protection of private data have emerged as top priorities. Legal protection for private data is governed by unique rules in several nations, but not in Indonesia. Information technology advancements and Indonesia's steadily rising internet service user base highlight the need for unique measures to safeguard private information and privacy in the country.

Although the ITE Law governs private data, it does not define what constitutes private data. Minister of Communication and Information Regulation No. 20 of 2016 concerning Protection of Private Data in Electronic Systems (Permenkoinfo 20/2016) and Government Regulation No. 18 of 2012 concerning Implementation of Electronic Systems and Transactions (PP 18/2012) both contain definitions for private data. Sector-specific implementing rules, like OJK Circular Letter No.014/SEOJK.07/2014, which addresses the security and confidentiality of consumer and/or private data (SEOJK 014/2014), are also included in this.

PP No.82/2012, one of the implementing rules required by the ITE Law, mandates electronic system operators to protect the integrity of private data and the agreement of the data owner before any private data can be acquired, used, disclosed, or utilized. However, PP No.82/2012 does not provide a more detailed reflection of the fundamental principles of protecting private data. The principles of protecting private data and more thorough regulation are included in Permenkoinfo No. 20/2016, which is a lower regulatory level. Permenkon-info No.20/2016 covers the protection of private data in electronic systems, including protection for its acquisition, collection, processing, analysis, storage, display, announcement, transfer, dissemination, and destruction. Sectoral implementing regulations also govern the protection of private data. For example, Bank Indonesia and the Financial Services Authority have regulations governing the protection of customer private data. Therefore, Indonesian laws pertaining to the protection of private data are still sectoral in nature.

At a lower regulatory level, Permenkoinfo No. 20/2016, the concepts of protecting private data and more thorough regulation are evident. Permenkon-Info No.20/2016's definition of private data protection in electronic systems covers safeguards against the acquisition, gathering, processing, analyzing, storing, displaying, announcing, transmitting, disseminating, and destroying private data. Sector-specific implementing regulations also govern the protection of private data. For example, Bank Indonesia and the Financial Services Authority have regulations governing the protection of customer private data. As a result, Indonesian laws pertaining to the protection of private data are yet sectoral.

Business actors are solely forbidden from offering, creating, and promoting false goods and/or services under Essay 9 of the Consumer Protection Law. The protection of consumer private data is not covered by these regulations. The Consumer Protection Law still contains gaps or inadequacies, which leads to business actors disregarding The privilege to privacy over customers' private information. As a result, consumers lack a solid legal foundation to ensure their right to privacy as consumers. Some of the aforementioned examples demonstrate that, despite the fact that the implementation of sector-specific private data protection has been governed by a number of legal regulations, specific regulations—that is, private data protection laws that can address cross-sectoral issues—remain necessary given the complexity and cross-sectoral reach of the business model of the digital economy. In addition to monitoring and safeguarding private data from abuse by the government and corporations, a specific institution must be established to handle consumer protection claims. This organization should also be able to raise public awareness in an effort to stop the misuse of private information. The Data Protection Authority, also known as the DPA, is a specific agency for the protection of private data inside the European Union that is responsible for overseeing the sharing of private information. Regarding the General Data Protection Regulation, often known as the GDPR, DPA is impartial and unaffiliated with either the public or commercial sectors. In light of the numerous organizations engaged in data collection and storage operations in Indonesia, the creation of a specialized institution to safeguard private data is imperative. Furthermore, everyone will be bound by the rules pertaining to private data, including those in the public, private, and governmental sectors. Consequently, it is ideal for this unique institution to be self-contained, have its own budget, and not be dependent on other organizations.

Current rules and regulations, such as the ITE Law, are thought to be inadequate in punishing the misuse of private data. The ITE Law's Essay 26 has made it clear that any use of information pertaining to an individual's private data through electronic media must be done so with the individual's consent and that anyone whose rights are violated may file a lawsuit. Regretfully, however, this standard does not specifically govern the procedures for the provisions that compel institutions to fulfill their duties to any institution that is assigned responsibility for doing so. This is the reason why there is a chance that private information will be misused. Since this clause is still in the form of a rubber Essay, it is easy to interpret widely and its bounds are unknown. Additionally, there are no legal repercussions (sanctions) for the institutions in question or the perpetrators themselves.[21]

Strict penalties are offered in the Private Data Protection section not only for data controllers but also for data processors and/or third parties who are found to have purposefully and illegally misused private data. In addition to criminal penalties, civil penalties are also imposed, with special attention paid to compensating for insignificant damages. Strong and enforceable penalties are required for state institutions as well as for interprivate and private/business disputes. There is no denying that the state has the ability to misuse private data, as seen in situations where it interacts with or enters into agreements with private companies. It is thought that the state's extensive data collection efforts run the risk of creating avenues for the state to abuse private information. Sadly, legislation pertaining to fines against governmental entities are not yet covered by Private Data Protection. Therefore, the author argues that if the state is serious about protecting private data, it must create legislation that include penalties for the state in the event that it violates the protection of private data. People

will feel safer from misuse of power or authority that uses people's (consumers') private information for partisan purposes in this way.

Now Indonesia has a policy or regulation regarding personal data protection which is regulated in the provisions of Law Number 27 of 2022 concerning Personal Data Protection. Regulations regarding this matter are still contained separately in several laws and regulations and only reflect aspects of personal data protection in general. Further regulations regarding the protection of internet users' personal data are contained in the ITE Law. ITE Law. It does not yet contain specific personal data protection rules. However, it is implicit in the ITE Law. raises a new understanding about the protection of the existence of electronic data or information, both public and private. The elaboration of personal electronic data is further mandated by the ITE Law in PP PSTE.[12]

Protection of personal data in an electronic system in the ITE Law includes protection from unauthorized use, protection by electronic system operators, and protection from illegal access and interference. Regarding the protection of personal data from unauthorized use, Article 26 of the ITE Law requires that the use of any personal data in electronic media must obtain the consent of the owner of the data concerned. Any person who violates this provision may be sued for losses incurred. In its explanation, Article 26 of the ITE Law states that personal data is part of a person's personal rights. Meanwhile, the definition of personal data can be seen in Article 1 PP PSTE, namely certain individual data that is stored, maintained and maintained as true and protected by confidentiality.

The explanation of article 26 paragraph (1) of the ITE Law also explains further the meaning of personal rights. The contents of the explanation are as follows: In the use of Information Technology, the protection of personal data is one part of personal rights (privacy rights). Personal rights contain the following meaning: 1) Personal rights are the right to enjoy private life and be free from all kinds of interference; 2) Personal rights are the right to be able to communicate with other people without spying; 3) Personal rights are the right to monitor access to information about a person's personal life and data; 4) If a general interpretation is taken, data protection has actually been regulated in the following articles in the ITE Law, namely in Articles 30 to Article 33 and Article 35 which is included in Chapter VII concerning Prohibited Actions. The ITE Law strictly prohibits unlawful access to other people's data through electronic systems to obtain information by breaking through security systems.(Tia Deja Pohan, 2023)

Even though it has been generally regulated in the ITE Law and in several other laws and regulations, Indonesia feels it is very necessary to immediately make special regulations regarding the protection of personal data. One of the main reasons is to increase Indonesia's economic value in international business relations. If Indonesia already has strict and adequate regulations, then developed countries such as the European Union or Singapore will no longer be reluctant to carry out business relations with Indonesian people via cyberspace, because in business relations an automatic transfer of data will be carried out, where the regulations are in place. Developed countries emphasize that data transfers can only be carried out to countries that have equally strong privacy protection.

Apart from economic reasons, privacy policies must be strengthened as part of human rights laws. Privacy is part of human rights and special arrangements regarding the protection of personal data are one way to respect this right.

In Indonesia, there is concern about protection for privacy and protection of personal data because until now there is no law that clearly and specifically regulates this matter. Therefore, privacy and personal data protection issues have become an urgent agenda in today's modern era. Many countries have implemented special regulations regarding legal protection for personal data, but this is not the case in Indonesia. The development of information technology and the continued increase in internet service users in Indonesia increasingly shows the need for special arrangements to protect privacy and personal data in Indonesia.

The ITE Law regulates personal data, but the ITE Law does not provide a definition of personal data itself. Personal data terminology is provided in regulations under laws including Government Regulation no. 18 of 2012 concerning Implementation of Electronic Systems and Transactions (PP 18/2012), Minister of Communication and Information Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (Permenkoinfo 20/2016). This also includes sectoral implementing regulations such as OJK Circular Letter No.014/SEOJK.07/2014 concerning Confidentiality and Security of Consumer Data and/or Personal Data (SEOJK 014/2014).[14]

As one of the implementing regulations mandated in the ITE Law, PP No.82/2012 imposes responsibility on electronic system operators to maintain the integrity of personal data and requires the data owner's consent to any acquisition, use, utilization and disclosure of personal data. However, PP No.82/2012 does not reflect the basic principles of personal data protection in more detail. The principles of personal data protection and more comprehensive regulation appear at a lower regulatory level, namely Permenkoinfo No. 20/2016. The scope of personal data protection in electronic systems in Permenkon-info No.20/2016 includes protection for the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination and destruction of personal data. Personal data protection is also regulated in sectoral implementing regulations, such as the protection of personal data for consumers which is regulated in Bank Indonesia and Financial Services Authority regulations. Thus, personal data protection regulations in Indonesia are currently still sectoral in nature. [15]

Consumers' personal data is very vulnerable to misuse considering that consumers' personal data is basically often linked when consumers use services or buy goods. For example, misuse of personal data due to promotions carried out by service providers/business actors for certain interests. Promotional actions are indeed regulated in Article 1 number 6 of the Consumer Protection Law but unfortunately the Consumer Protection Law itself does not regulate provisions prohibiting promotional activities that use consumer personal data without the permission/approval of the person concerned. Article 9 of the Consumer Protection Law only prohibits business actors from offering, producing, advertising goods and/or services that are not true. These provisions do not touch on the protection of consumer personal data. Therefore, consumers do not have a strong legal basis to guarantee their right to privacy as consumers, so the Consumer Protection Law still has empty spaces or loopholes and causes business actors not to respect the right to privacy over consumers' personal data. Some of the things above show that although the implementation of personal data protection on a sectoral

basis has been regulated in several legal regulations, special regulations are still needed, namely personal data protection laws that can solve cross-sectoral problems, considering that the digital economy business model is complex and cross-sectoral in scope. The establishment of a special institution is needed not only to monitor and protect personal data from misuse by both corporations and the government, but is also tasked with handling consumer protection disputes. In efforts to prevent misuse of personal data, this institution is also expected to be able to encourage public awareness. As a comparison, the European Union already has a special agency for personal data protection (Data Protection Authority or DPA) which is tasked with supervising the exchange of personal data. Referring to general data protection regulations (General Data Protection Regulation or GDPR), DPA is independent and not affiliated with the government or any private party. In this regard, the establishment of a special institution to protect personal data is very necessary considering that there are many entities involved in data collection and storage activities in Indonesia. Moreover, regulations regarding personal data will be binding on all parties, both from the public, private and government sectors. Therefore, it is best for this special institution to be independent and have its own budget and not be tied to other institutions.

Existing laws and regulations are considered not optimal in providing sanctions for misuse of personal data, for example the ITE Law. Article 26 of the ITE Law has emphasized that the use of any information via electronic media that concerns a person's personal data must be carried out with the consent of the person concerned and that any person whose rights are violated can file a lawsuit, but unfortunately this norm does not regulate in detail the mechanism for the provisions that require institutions to any institution that is given responsibility as an assignment to carry out these obligations. This is what causes the potential for misuse of personal data to occur. There are no legal consequences (sanctions) for the institutions responsible and for the violators themselves, this provision is still in the form of a rubber article so it is easy to interpret broadly and the boundaries are unclear.

Meanwhile, in Personal Data Protection, strict sanctions are provided not only for data controllers but also data processors and/or third parties who are proven to have intentionally and unlawfully misused personal data. The sanctions given are not only criminal but also civil, even compensation for immaterial losses is emphasized. Firm and binding sanctions are needed not only for interpersonal, private/corporate conflicts but also for state institutions. It cannot be denied that the potential for misuse of personal data can also be carried out by the state, for example in cases where the state deals with or enters into work agreements with private parties. Massive data collection carried out by the state is considered to be at risk of opening up opportunities for misuse of personal data by the state. Unfortunately, Personal Data Protection does not yet accommodate sanctions regulations against state institutions. Therefore, according to the author, if the state is committed to providing personal data protection, the state needs to make regulations in which there are sanctions for the state if the state violates the protection of personal data. In this way, people will feel protected from abuse of authority or power that involves using people's (consumers') personal data for one-sided interests.

4 Conclusion

Protecting private information is a human right and a component of privacy. This acknowledgement is expressed in the constitution as well as in a number of legal rules. Nevertheless, there are no laws that expressly govern the statutory degree of private data protection. As of right now, Indonesia has no laws governing the use of private information in online transactions. Only Essay 26 and a few other paragraphs of the ITE Law control this matter. For internet consumer transactions to be facilitated, customers must have legal protection. Regardless of the medium used, the goal is to enforce all transactions uniformly. It is crucial to eliminate current legal barriers and handle significant new challenges pertaining to electronic media. The state must fulfill its obligation to protect each person's private information as a means of acknowledging, upholding, and defending their human rights, as stipulated by the Republic of Indonesia's 1945 Constitution, given the existence of contributing factors and the consequences of misuse. Consequently, the role In the age of the digital economy, the state can safeguard consumer private information by enacting distinct laws pertaining to data protection, creating specialized organizations to safeguard private information, and enforcing stringent penalties.

In the digital age, safeguarding customer private information is crucial and should be implemented right away. Private data has become a valuable commodity as a result of the advent of the digital era and the phenomenon and potential of big data. Given that the growth of the digital economy has been shown to promote economic expansion, this is not without justification. The protection of consumer private data is still subpar despite its tremendous economic worth. As data owners, consumers are concerned about the widespread misuse of private data that still occurs.

References

[1] R. Belwal, R. Al Shibli, and S. Belwal, "Consumer Protection and Electronic Commerce in the Sultanate of Oman," *J. Inf. Commun.*, vol. 19, no. 1, pp. 38–60, 2020, doi: 10.1108/JICES-09-2019-0110.

[2] R. A. Bahtiar, "Potensi, Peran Pemerintah, dan Tantangan dalam Pengembangan E-Commerce di Indonesia [Potency, Government Role, and Challenges of E-Commerce Development in Indonesia]," *J. Ekon. dan Kebijak. Publik*, vol. 11, no. 1, pp. 13–25, 2020, doi: 10.22212/jekp.v11i1.1485.

[3] R. Aswandi, P. R. N. Muchsin, and M. Sultan, "Perlindungan Data dan Informasi Pribadi melalui Indonesian Data Protection System (IDPS)," *J. Legis.*, vol. 3, no. 2, pp. 167–190, 2020, [Online]. Available: https://journal.unhas.ac.id/index.php/jhl/article/view/14321

[4] M. R. Anjani and B. Santoso, "Urgensi Rekonstruksi Hukum E-Commerce di Indonesia," *J. Law Reform*, vol. 14, no. 1, pp. 89–103, 2018, doi: https://doi.org/10.14710/lr.v14i1.20239.

[5] T. D. Pohan and M. I. P. Nasution, "Perlindungan Hukum Data Pribadi Konsumen Dalam Platform E Commerce," *Sammajiva J. Penelit. Bisnis dan Manaj.*, vol. 1, no. 3, pp. 42–48, 2023, [Online]. Available: https://e-journal.nalanda.ac.id/index.php/SAMMAJIVA/article/view/336

[6] L. Sautunnida, "Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris Dan Malaysia Urgency of Personal Data Protection Law in Indonesia; Comparative Study of English and Malaysia Law," *Kanun J. Ilmu Huk.*, vol. 20, no. 2, pp. 369–384,

2018.
[7] K. dan K. W. Dimyati, “Metode Penelitian Hukum,” Surakarta: Universitas Muhammadiyah Surakarta, 2015.
[8] K. Wardiono and K. Dimyati, *Metode Penelitian Hukum*. Surakarta: Fakultas Hukum Universitas Muhammadiyah Suraka, 2004.
[9] T. P. Kurnianingrum, “Urgensi Perlindungan Data Pribadi Konsumen di Era Ekonomi Digital,” *Kajian*, vol. 25, no. 3, pp. 197–216, 2020, doi: 10.22212/kajian.v25i3.3893.
[10] Y. Marpi, R. S. Dewi, M. Maisa, and S. Naim, *Legal Consequences of Takeover of Authority in Mineral and Coal Mining by the Ministry of Energy and Mineral Resources of the Republic of Indonesia*, no. Icclb. Atlantis Press SARL, 2023. doi: 10.2991/978-2-38476-180-7_158.
[11] M. Rustam, “Internet dan Penggunaannya (Survei di Kalangan Masyarakat Kabupaten Takalar Provinsi Sulawesi Selatan),” *J. Stud. Komun. dan Media*, vol. 21, no. 1, pp. 13–24, 2017, doi: 10.31445/jskm.2017.210102.
[12] S. Dewi Rosadi and G. Gumelar Pratama, “Urgensi Perlindungandata Privasidalam Era Ekonomi Digital Di Indonesia,” *Verit. Justitia*, vol. 4, no. 1, pp. 88–110, 2018, doi: 10.25123/vej.2916.
[13] R. A. Nugraha, “Perlindungan Data Pribadi dan Privasi Penumpang Maskapai Penerbangan pada Era Big Data,” *Mimb. Huk. - Fak. Huk. Univ. Gadjah Mada*, vol. 30, no. 2, p. 262, 2018, doi: 10.22146/jmh.30855.
[14] S. Dewi, “Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia,” *Yust. J. Huk.*, vol. 5, no. 1, pp. 22–30, 2016, doi: 10.20961/yustisia.v5i1.8712.
[15] M. Indriyani, “Perlindungan Privasi dan Data Pribadi Konsumen Daring Pada Online Marketplace System,” *Justitia J. Huk.*, vol. 1, no. 2, 2017, doi: 10.30651/justitia.v1i2.1152.
[16] A. Pujianto, A. Mulyati, and R. Novaria, “Pemanfaatan Big Data Dan Perlindungan Privasi Konsumen Di Era Ekonomi Digital,” *Maj. Ilm. Bijak*, vol. 15, no. 2, pp. 127–137, 2018, doi: 10.31334/bijak.v15i2.201.
[17] Rista Maharani; Andria Luhur Prakoso, “Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection of Consumer Personal Data by Electronic System Providers in Digital Peningkatan substansial dalam penggunaan platform e-commerce di Indonesia telah,” *J. Usm Law Rev.*, vol. 7, no. 1, pp. 333–347, 2024.
[18] B. H. Mantri, “Perlindungan Hukum Terhadap Konsumen Dalam Transaksi E-Commerce,” *Law Reform*, vol. 3, no. 1, p. 1, 2007, doi: 10.14710/lr.v3i1.12340.
[19] A. Shandy Utama, “Law Enforcement to Copyright Infringement of Songs on the Internet Media,” *FIAT JUSTISIAJurnal Ilmu Huk.*, vol. 12, no. 3, p. 234, 2018, doi: 10.25041/fiatjustisia.v12no3.1211.
[20] A. L. S. Siahaan, “Urgensi Perlindungan Data Pribadi di Platform Marketplace terhadap Kemajuan Teknologi (Urgency of Personal Data Protection on Marketplace Platforms Against Technological Advances),” *Maj. Huk. Nas.*, vol. 52, no. 2, pp. 209–223, 2022, doi: 10.33331/mhn.v52i2.169.
[21] Julisar and E. Miranda, “Pemakaian E-Commerce untuk Usaha Kecil dan Menengah guna Meningkatkan Daya Saing,” *ComTech*, vol. 4, no. 2, pp. 638–645, 2013.