International Journal of Research in Engineering, Science and Management
Volume 6, Issue 1, January 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Review of Legal Weakness on Protection of Personal Data in Online Transactions on Consumer-to-Consumer Concept in E-Commerce

Tubagus Muhammad Ali Ridho Azhari[1*], Maria Grasia Sari Soetopo[2]
[1,2]*Department of Law, University of Pelita Harapan, Tangerang, Indonesia*

***Abstract*: The need for legal protection guarantees for digital concepts is very much needed in the digitalization era, especially with the widespread use of the internet in Indonesia, which tends to increase to become very vulnerable to opportunities for criminal acts to occur, especially law enforcement on personal data leaks. There have been several cases of personal data leakage in several e-marketplaces in Indonesia. The existence of vulnerabilities in the e-commerce cyber security system in Indonesia against personal data leakage requires the government to resolve law enforcement issues through the ratification of Law No. 27 of 2022 concerning the Protection of Personal Data as a legal umbrella if there is a problem of leakage of personal data to every citizen as an e-commerce user. This study aims to review "weaknesses in the law" on protecting personal data in online transactions on the concept of "consumer to the consumer in e-commerce". This review research uses a normative legal evaluation approach and normative-empirical law with qualitative analysis. This study found that personal data protection regulations are still partial, so Law no. 27 of 2022 concerning the Protection of Personal Data does not yet have maximum legal force purely as a legal regulator for guaranteeing personal data security.**

***Keywords*: Data protection, Indonesian E-Commerce transactions, Indonesian legal regulation, Personal data.**

1. Introduction

The importance of personal data protection begins to strengthen along with the increasing number of internet users. There have been several cases, especially those related to using and disseminating personal data and leading to fraud or criminal acts. With so many problems with personal data leakage, the government took action to submit proposals with a priority scale in the national legislative program for the personal data protection bill to the Indonesian Parliament, which had been proposed by the government to be discussed starting in 2017 and only passed in 2017. September 2022 and promulgated in October 2022 so that this is one way out of making legal rules to protect personal data. The protection of personal data is very closely related to the concept of privacy, so the concept of privacy itself is an idea of maintaining personal integrity and dignity [1]. Personal data is an asset or commodity with high economic value. In addition, there is a correlation between the level of trust and the protection of certain data from personal life [2].

Some time ago, some problems occurred in Indonesia related to personal data being leaked onto social media, even to the point where some traded Indonesian people's data on one of the buying and selling internet sites to seek profit from the sale of personal data. According to data from the Association of Indonesian Internet Service Providers, in 2021, there was an alleged leak similar to BPJS Health data, which totalled 270 million Indonesian people's data. Personal information in the leaked data included NIK (residential identification number), name, address, and telephone number. It was even reported that the salary amount was also included and included a million data samples for checking, which later the personal data was sold with material losses allegedly reaching Rp. 600 trillion. Then, in the alleged case of data leakage belonging to BRI Life participants, as many as 2 million customers' data were suspected of being traded in cyberspace, and hackers successfully retrieved as many as 463,000 documents. The case of data leakage so that the data is traded is a severe problem in Indonesia. With rapid technological advances, adjustments to technology in regulation must keep pace with current developments so that the need for regulation as a legal umbrella for personal data protection is urgently needed.

In 2019, 13 million Bukalapak user accounts were hacked by hackers from Pakistan. Bukalapak has indeed confirmed that there was a hacking attempt on its website. However, Bukalapak claims that no essential data and personal information were obtained, such as user passwords or financial data. Then, in July 2020, the Indonesian Cyber Research Institute for Communication and Information System Security Research Center (CISSReC) found that someone had purchased the data of 91 million Tokopedia e-commerce account users, which was leaked several times last May by circulating the download link via Facebook [3]. In October 2020, it was recorded that 1.1 million user data of Lazada's RedMart online supermarket were hacked. Much personal information is traded, such as names, telephone numbers, e-mails, addresses, and passwords, to credit card numbers of RedMart users. Lazada party justifies attempts to steal user data. Lazada said the data was stolen from a RedMart database hosted by a third-party

*Corresponding author: aliridhoazhari@gmail.com

service provider.

Nonetheless, Lazada claims the data stolen by hackers is expired data. Then in the same year, there was a hacking of one of the e-commerce in Indonesia by hacking the account registered with the e-commerce with an estimated 91 million accounts and 7 million merchant accounts. Almost all e-commerce accounts have their data taken by hackers, then sell the data on the dark web in the form of User ID, e-mail, full name, date of birth, gender, and cellphone number and password, which is still encrypted at a price of around Rp. 74 million or about $ 5,000. However, e-commerce then claims and checks that user payment data, such as debit cards, and credit cards are still secure and states that the security of personal data is a top priority [4].

With the increase in e-commerce users, it is accompanied by the development of the technology used so that the vulnerability to online marketplaces (e-commerce) is an essential record for security in terms of service user data because it does not rule out the possibility of data hacking carried out by other people - those committed by e-commerce site hackers [5]. The danger occurs when there is a data leak, and it spreads widely to be traded, and then the data can be used to commit criminal acts or even other criminal acts, so it can interfere and create anxiety or comfort for the owner of the data. Therefore, with the misuse of personal data, it can be seen that there are system weaknesses and a lack of supervision, so personal data can be misused, resulting in losses for the data owner.

Misuse, theft, and sale of personal data is a violation of law in the field of information technology and is categorized as a violation of human rights because it does not get approval from the owner of the data to be used and traded through internet sites because they only want to gain profit by harming other people's rights and data. Privacy is part of human rights that must be protected [6], [7].

Based on the problem of personal data leakage through e-commerce sites. Vulnerabilities in the security system are inconvenient for a person or consumer as a user to make transactions that result in the leaking of the user's data. According to a survey by katadata.co.id, the trend of e-commerce users continued to grow between 2017 - 2023.

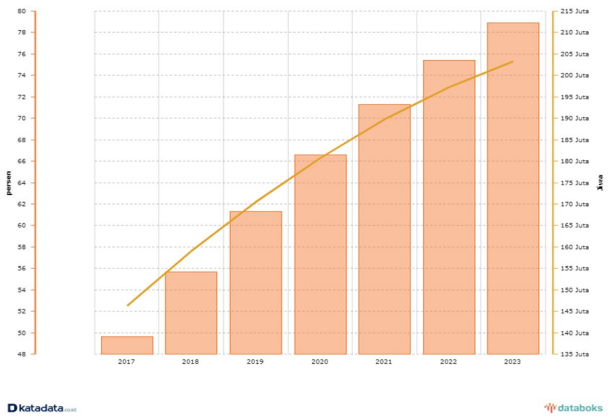

Fig. 1. Users and Penetration Rate of E-Commerce in Indonesia
Source: katadata, 2022

The trend of e-commerce users in Indonesia has grown quite large in recent years. It is predicted that growth will continue in the next few years. Statista noted that the number of e-commerce users in Indonesia in 2017 reached 139 million users, then rose 10.8% to 154.1 million users last year, so this year it is projected to reach 168.3 million users and 212.2 million in 2023. Therefore, the same thing happens with the penetration rate of e-commerce which is continuously increasing until 2023 and is projected to reach 75.3% of the selected market population. Thus, it is necessary to pay attention to these predictions on the growing trend of e-commerce use regarding the form of guarantees in the cyber security system owned by each e-commerce.

According to the problems, there is a vulnerability in the e-commerce cyber security system in Indonesia to leakage of personal data, which requires the government to have solutions to law enforcement problems for legal weaknesses, therefore recently, the Government and the Indonesian Parliament agreed to ratify Law No. 27 of 2022 concerning the protection of personal data as a legal regulator if there is a problem of leakage of personal data as an effort to provide guarantees and legal protection to every citizen as an e-commerce user where buying and selling transactions occur, this study aims to review "weaknesses in the law" on the protection of personal data in online transactions on the concept of "consumer to the consumer in e-commerce"

2. Method

This research is a review of research related to law regulation in Indonesia. This research uses descriptive-evaluative with a qualitative approach. Evaluative research is research that evaluates a program, activity, theory, or findings to measure an activity, program, and research through activities to compare the results of previous theories [8], [9].

The evaluative descriptive used in this study is to evaluate theory and legal data in Indonesia. These previous studies and laws were searched using the Google search engine on the websites of the constitution of the Republic of Indonesia, Google Books, Google Scholar, and ScienceDirect. A qualitative approach in this study is used to interpret the results of evaluating legal weaknesses related to e-commerce data protection as a theoretical basis as a guide so that the research focus follows the reading of the case study. According to [10], qualitative research contains information about the main phenomena being explored in a study, research participants, and research locations. Qualitative research begins in the field based on empirical facts, not theory. Data and information obtained from the case study area are taken for meaning and concept, presented in an analytical descriptive manner and generally without using numbers because it prioritizes processes in the case study area.

This research was conducted in 2022 using the results of a survey of data on laws in Indonesia related to consumer data protection. This data was obtained from the book of the constitution of the Republic of Indonesia. All these data will be evaluated based on previous findings or theories. The laws regarding consumer protection found in the evaluation are based on the theoretical basis and prior research findings. The

results of this evaluation are read descriptively regarding how legal protection is for consumers who use e-commerce in Indonesia and the weaknesses and legal policies in Indonesia.

3. Result and Discussion

A. Personal Data Protection Policy in Indonesia

To protect private data, respect for the right to privacy must begin by providing legal certainty. Therefore, guarantees for the protection of privacy data must be placed in a legal instrument with the highest power, namely the constitution, because the Constitution or the Constitution is the highest legal instrument in a country. Legal certainty (legality principle) is necessary and cannot be ruled out in the context of law enforcement by every nation.

The government seeks to carry out its obligations based on the 1945 Constitution that guaranteeing and protecting its citizens is the state's responsibility. Regarding the protection of personal data, currently, several laws and regulations are still in use which become the legal umbrella for legal protection against the misuse of personal data which leaks out to the public. Based on the provisions of laws and regulations, the legal umbrella that forms the basis is Law No. 27 of 2022 concerning the protection of Personal Data, Law no. 11 of 2008 Jo. Law No. 19 of 2016 concerning Information and Electronic Transactions and Law no. 23 of 2006 Jo. Law No. 24 of 2013 concerning Population Administration and Law no. 39 of 1999 concerning Human Rights.

B. E-commerce Privacy Policy

The privacy policy is used to inform how a website manages information for visitors and users regarding what information will be retrieved and used and how the online marketplace system works. Each online marketplace has a privacy policy that aims to provide legal certainty over guarantees for data protection for visitors or users who use the website, especially in terms of transactions. Then, the privacy policy is an obligation in the form of transparency for online marketplaces to collect and process personal user data to provide guarantees and convenience in online transactions for consumers (sellers - buyers) who use third-party facilities, in this case, the online marketplace.

In addition to the objective of the online marketplace's obligation to create a privacy policy, there are also significant benefits for e-commerce activities for the parties if carried out and adhered to as compliance measures properly by both parties, namely:

a) Increase the sense of security and trust between online consumers and e-commerce providers.
b) Protection of privacy rights for online consumers in their e-commerce activities.
c) Creating a fair business competition climate in every electronic transaction activity.
d) There is an appropriate legal settlement following the agreed-upon privacy policy if, in the future online consumers have their privacy rights violated.

This regulation is a benefit form for the parties conducting the transaction as a legal relationship to obtain comfort and guarantees for a transaction. This step is related to marketplace system transactions in Indonesia with violations of privacy rights experienced by consumers in the online marketplace system. It takes preventive or careful steps from consumers to include their private data because consumer privacy rights are violated when the company processes consumers' data. So far, there have been forms of public complaints reported to the e-business directorate, the Ministry of Communication and Informatics, mostly related to discrepancies between the goods ordered and the goods received. For cases related to privacy rights, there have been no reports of complaints, so legal protection guarantees for consumers cannot be accommodated well.

C. Personal Data Protection Regulations

Personal data in e-commerce transactions is necessary to verify accounts used to carry out electronic transactions. However, in its implementation in carrying out law enforcement against cases of leakage of personal data, which results in the sale of personal data on specific sites, it will get terrible problems due to the inconvenience caused to someone who has leaked their data.

There is a risk that occurs when personal data is leaked and used by irresponsible people who tend to commit crimes by utilizing personal data, including First, personal data can be used to break into financial accounts. This case is done using social manipulation by tricking the victim. For example, perpetrators can send e-mails with important or manipulative messages so that victims provide personal data and include bank services in a link or attachment. Second, using personal data against online loan fraud is illegal. In general, borrowing money is done by other people pretending to be the data owner. The actual data owner doesn't even know about the lending problem, so they get poor treatment in the form of terror to make a refund, including interest. Third, leaked personal data of residents can be used to map the profile of the data owner – for example, for political purposes or advertisements on social media. Data leaks like this can be used to map users' political preferences, which can then be used as targets for disinformation. Fourth, hacking social media account data can also be used for various acts of online extortion.

The potential for data leakage is not only in electronic transactions used for criminal acts but in other transactions. There is also a tendency when there is leakage of personal data as another crime. As a condition for conducting transactions, e-commerce is fully responsible for data leaks that occur. Hence, the role of e-commerce in maintaining data confidentiality is also necessary as government participation in its business so that there is a safe and comfortable atmosphere in conducting every transaction electronically.

D. Legal Implementation of Legal Protection Regulations of Personal Data

Currently, Indonesia already has Law No. 27 of 2022 concerning Protection of Personal Data, with the aim of combining privacy regulations on scattered personal data into a

separate law with the objective of providing boundaries between rights and obligations regarding the acquisition and use of personal data but based on the general explanation of the Act - Invite No. 27 of 2022 concerning Personal Data Protection states that in relation to overlapping regulations, the Personal Data Protection provisions are a standard for Personal Data Protection in general, whether processed in part or in whole by electronic and non-electronic means, where each sector can apply Protection Personal Data in accordance with the characteristics of the sector for which Personal Data Regulation aims, among other things, to protect and guarantee the fundamental rights of citizens related to personal self-protection, guaranteeing the public to get services from Corporations, Public Agencies, International Organizations and the Government, encouraging the growth of the digital economy and the information technology industry and communications, and support the improvement of domestic industrial competitiveness.

E. Data Protection Guarantee in E-commerce Transactions

Article 58 paragraph (2) Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems explains that the bearer of the mandate is the controller of personal data following its designation for storing and using personal data referring to personal data protection standards according to propriety and developing business practices. If a business actor violates these provisions, he will be subject to Article 80 paragraph (1) of Government Regulation No. 80 of 2019 concerning trading through electronic systems only in the form of administrative sanctions for these violations. Guarantees for legal protection and certainty also cannot be applied to criminal sanctions because this is a measure of law enforcement that uses based on positive law in Indonesia.

The obligations for personal data users are also regulated based on articles 27 and 28 of the Minister of Communication and Informatics No. 20 of 2019 concerning protecting Personal Data in Electronic Systems. There is an obligation as a form of compliance for business actors, in this case, e-commerce, in carrying out their business.

Based on these two articles, business actors must carry out the obligations as the regulations are made so that, as an application of the law, it applies to parties interested in using personal data in e-commerce. In addition, e-commerce must comply with regulations made by the government in conducting transactions because everyone, between sellers and buyers who conduct transactions in e-commerce, must be obliged to fill in personal data according to KTP. Parties working online transactions through an online marketplace system are required to fill in personal data because this obligation is a form of an absolute requirement made by the online marketplace.

F. Comparison of Personal Data Protection Laws with Other Countries

In protecting and providing legal guarantees for personal data, several other countries also have regulations related to the protection of personal data because online transactions are increasingly developing and advanced, requiring other countries to have rules to ensure the security of their citizens' data. Several regulations in several countries have become a reference for the making of Law No. 27 of 2022 concerning Personal Data Protection in Indonesia.

G. Settlement of Personal Data Protection Disputes

Without institutional authority, legal guarantees, protection, and certainty cannot be fulfilled. Thus that, law enforcement measures on criminal sanctions cannot be applied based on the provisions of Law No. 27 of 2022 concerning the protection of personal data if there are similar cases or cases of data leakage

Table 1
Protection of personal data in several countries

No.	Country	Information
1	European Union	The European Union has rules for protecting personal data, namely the General Data Protection Regulation (GDPR) based on the Directive on the Protection of Personal Data (95/46/EC), which is a guideline for establishing laws regarding data protection for European Union countries [2] In developing the latest legal provisions regarding data protection in the European Union, namely EU 679/2016 Regulation The Protection of Natural Persons concerning The Processing of Personal Data and on The Free Movement of Such Data (General Data Protection Regulation [11]. These provisions protect citizens' personal data against data misuse by private parties or companies within the European Union or foreign companies that use citizens' data within the European Union, and these rules apply universally to companies. European Union and foreign companies located in the European Union [12].
2	United States of America	Based on the US Privacy Act 1974, the United States Department of Health 1973 put forward the general principles of personal data protection contained in Fair Information Practices, which consist of 5 basic principles. Based on the Privacy Act of 1974 emphasized restrictions on the collection of personal information by federal government agencies. However, the law does not apply to collecting personal data by private institutions.
3	Japan	The Act on the Protection of Personal Information (APPI) regulates personal data protection in Japan. APPI is the rule used in the elaboration following the amendments made in 2017 [13]. Previously, Japan had had personal data privacy protection regulations since 2000. The Data Protection Art is the rule of law adopted by the Federal Government of Japan. The Keidanren, the representative body that specifically regulates industrial and trade issues in Japan, formulated legal rules related to the privacy protection of personal rights. The Data Protection Art was born to regulate personal data as a form of protection for the Japanese government in the era of trade competition in the European Union.
4	Hong Kong	Hong Kong became the first country to comprehensively regulate privacy issues regarding personal data in Asia, namely the Personal Data Privacy Ordinance of 1995 (PDPO), which made significant changes in 2012. a particular institution that deals with issues of personal data privacy, namely the Privacy Commissioner for Personal Data (PCPD). Then, in carrying out and implementing these regulations, the Hong Kong government established a very broad Personal Data Privacy Commissioner, including overseeing and promoting PDPO compliance.
5	Singapore	Personal data protection in Singapore is also contained in the Personal Data Protection Act (PDPA), which was recently amended in 2020. The law was created as a basic standard for data protection in the private sector. The goal is to increase confidence in data management and processing. For privacy data protection practices in Singapore, the Personal Data Protection Commission (PDPC) was presented in carrying out the enforcement and effectiveness of this rule.

committed by e-commerce parties, whether intentional or unintentional.

4. Conclusion

In enforcing the law against leakage of personal data, it must be accompanied by appropriate regulations or regulations that can accommodate any leakage of personal data as a form of guarantee for legal protection. In the C2C (Consumer to Consumer) concept in online transactions, the things that must be considered are the provisions or regulations regarding guarantees, and regulations are internal e-commerce rules as compliance with security guarantees that personal data from account owners in e-commerce is not leaked. In Indonesia, guarantees for the protection of personal data have just been accommodated through Law no. 27 of 2022 concerning the protection of personal data. However, this regulation has not been able to run optimally because it has just been promulgated, which has to be adjusted to other regulations in approximately two years, so this law will be optimally effective for only two years to come. After the enactment of Law No. 27 of 2022 concerning the protection of Personal Data if there is a misuse of personal data in e-commerce, for now, only administrative sanctions can be imposed. They cannot be subject to criminal sanctions if there is a misuse of personal data because implementing regulations have not been made for this law.

Regulations on personal data protection are still partial because there are still other regulations governing them. For this reason, Law no. 27 of 2022 concerning personal data protection does not yet have maximum legal force as a regulation to guarantee the security of personal data if there is a data leak by a third party. For this reason, other legal remedies are needed to regulate it, such as Government Regulation No. 71 of 2019 concerning the implementation of electronic systems and transactions and also the minister of communication and information regulation No. 20 of 2016 concerning the protection of personal data in electronic systems as a legal umbrella for guaranteeing the security of personal data protection.

The guarantee of the security of personal data protection in Indonesia is still not optimal because the implementation of personal data protection regulations is not optimal these regulations are still partial, and other legal remedies are still needed in dealing with the problem of leakage of personal data in Indonesia. The current government has not made derivative regulations formal regulations because Law no. 27 of 2022 concerning the protection of personal data is still material in general, even though there are administrative sanctions if there is a data leak.

The C2C concept through e-commerce with guaranteed personal data security is also not optimal in its implementation. Based on Government Regulation no. 80 of 2019 concerning Trading Through Electronic Systems is a legal basis for online marketplaces in carrying out their business actions these business actors are also part of the collection and processing of consumers' data in their online transaction activities. So that compliance with online marketplaces must follow these Government Regulations in ensuring the continuity of the security of personal data for each consumer in the context of buying and selling transactions. However, the problem with government regulation No. 80 of 2019 concerning trading through electronic systems is that it does not specifically regulate criminal sanctions. It only regulates administrative sanctions so that problems with leakage of personal data cannot be resolved optimally if data leak cases are repeated, which can be fatal for consumer convenience in buying and selling transactions online on online marketplaces.

References

[1] Djafar W, Komarudin A. Perlindungan Hak Atas Privasi di Internet-Beberapa Penjelasan Kunci. Elsam, Jakarta. 2014.
[2] Makarim E. Pengantar hukum telematika: Suatu kompilasi kajian. 2006.
[3] Indiana Malia. Sebelum BPJS Kesehatan, Ini 3 Kasus Kebocoran Data Konsumen E-commerce. IDN Times [Internet]. 2021; Available from: https://www.idntimes.com/business/economy/indianamalia/selain-bpjs-kesehatan-ini-3-kasus-kebocoran-data-konsumen-e-commerce/2
[4] Febyastuti E. Telaah hukum pidana Islam terhadap pencurian data pribadi konsumen E-commerce.
[5] Kaushik D, Gupta A, Gupta S. E-commerce security challenges: A review. In: Proceedings of the international conference on innovative computing & communications (ICICC). 2020.
[6] Rohendi A. Perlindungan Konsumen Dalam Transaksi E-Commerce Perspektif Hukum Nasional dan Internasional. J Ecodemica J Ekon Manaj dan Bisnis. 2015;3(2):474–88.
[7] Hariyono AG, Simangunsong F. Perlindungan hukum korban pencurian data pribadi (phishing cybercrime) dalam perspektif kriminologi. Bur J Indones J Law Soc Gov. 2023;3(1):428–39.
[8] Putra DW, Hidayat HP. Filsafat Ilmu Terkait Dengan Perencanaan Wilayah Dan Kota (Studi kasus: Green Urban Open Space dan Quality of Life). J Pengemb Kota. 2017;5(2):112–20.
[9] Putra RDW, Indradjati PN. Studi Deskriptif – Evaluatif Bentuk Tipologi Kawasan (Pembelajaran dari Kota Surabaya). J Pengemb Kota. 2022;2.
[10] Raskind IG, Shelton RC, Comeau DL, Cooper HLF, Griffith DM, Kegler MC. A review of qualitative data analysis practices in health education and health behavior research. Heal Educ Behav. 2019;46(1):32–9.
[11] Tsamara N. Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. J Suara Huk. 2021;3(1):60.
[12] Ramadhani SA. Komparasi Pengaturan Perlindungan Data Pribadi di Indonesia dan Uni Eropa. J Huk Lex Gen. 2021;3(21):78.
[13] Palito J, Soenarto SA, Raila TA. Urgensi Pembentukan Pengaturan Perlindungan Data Pribadi Di Indonesia Serta Komparasi Pengaturan Di Jepang Dan Korea Selatan. J Supremasi Huk. 2021;17(1):28.