Protection of Personal Data in Transactions Using E-Commerce in the Perspective of Indonesian Law (An Overview)

Tubagus Muhammad Ali Ridho Azhari*, Maria Grasia Sari Soetopo
Department of Law, University of Pelita Harapan, Indonesia
**Corresponding Author*

***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. Because of this phenomenon, this study aims to evaluate the protection of personal data in transactions using e-commerce from the perspective of Indonesian law. This study 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, E-Commerce transactions, Indonesia, Legal regulators, Personal data**

I. INTRODUCTION

Guaranteed legal protection is needed in the digitalization era. This reason happens because internet use in Indonesia tends to increase. Many internet users provide opportunities for crime to occur on the internet in the form of traded personal data. It is because, in the digitalization era, access to everything can be done using the internet. Therefore, data protection is needed for internet users. [1], [2].

In the concept of protection, the state's role has a goal to be realized in the form of protection, one of which is crucial is the protection of the personal data of every resident or citizen of Indonesia. As a form of innovation, information technology can now collect, store, share and analyze data. Thus, these activities have resulted in various sectors of life utilizing information technology systems, such as terms of using electronic commerce (e-commerce) in the trade/business sector, electronic education (e-education) in the education sector, electronic health (e-health) in the health sector, electronic Government (e-government) in the government sector, search engines, social networks, smartphones and mobile internet as well as the development of the cloud computing industry [2].

The increasing number of internet users strengthens the importance of protecting personal data. A number of cases have occurred, especially those related to using and disseminating personal data and leading to fraud or criminal acts [1]. With so many problems with personal data leakage, the Government took action to submit proposals with a priority scale in the National Legislative Program (Prolegnas) 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 importance of a regulation related to protecting public personal data is a mandate from Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states that: "Everyone has the right to protection of himself/herself, family, honor, dignity, and property under his control, and has the right to feel safe and protected from threats of fear to do or not do something that is a human right."

The issue of the importance of protecting personal data arises because of several violations against misuse of personal data that individuals and legal entities can experience. The protection of personal data is currently regulated through a separate law. However, it still takes up to 2 years in terms of adjusting its application until the adjustment of derivative regulations is based on the transitional provisions concerning Personal Data Protection which reads: "When this Law comes into force, Personal Data Controllers, Personal Data Processors, and other parties related to the processing of Personal Data, must comply with the provisions for processing Personal Data based on this Law no later than 2 (two) years after this Law was promulgated" [3].

Based on the Minister of Communication and Informatics Regulation No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems is a set of implementing regulations from Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, which mandates that guidelines for the protection of personal data in electronic systems to be further regulated in the Minister of Communication and Informatics regulations. Personal data is individual data that is stored, cared for, safeguarded, and protected confidentially [3]. As for specific

individual data, it is accurate and factual information that is attached and identifiable, either directly or indirectly, to each individual whose utilization is following the provisions of the laws and regulations [4].

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 APJII (Association of Indonesian Internet Service Providers), in 2021, there was an alleged leak similar to BPJS Health data, which totaled 270 million Indonesian people's personal 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' personal data were suspected of being traded in cyberspace, and hackers successfully retrieved as many as 463,000 documents. The case of data leakage that the data is changed 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 there were several cases of data leakage at e-commerce service providers in Indonesia. Pakistani hackers hacked 13 million Bukalapak user accounts. 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 [5]. 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, emails, 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 service provider.

Nonetheless, Lazada claims the data stolen by hackers is expired data [5]. Then in the same year, there was a hacking of e-commerce in Indonesia by hacking accounts registered with 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, email, full name, date of birth, gender, cellphone number, and password, which is still encrypted at a price of around Rp. 74 Million or about $ 5,000. However, the 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.

With the increase in e-commerce users and technological developments causing vulnerabilities to online marketplace (e-commerce) users, so that it becomes a record of data security for service users. User data security is essential because of the possibility of data hacking by e-commerce site hackers. The danger that occurs when data is leaked, spread widely, and traded, is that the data can be used to commit crimes, and the impact can be disturbing and troubling for the data owner. Misuse of personal data can occur due to system weaknesses and lack of supervision, resulting in losses for the data owner. Misuse, theft, sale of personal data are classified as violations of information technology law and human rights because the user does not obtain the consent of the owner of the data to be misused, disseminated, or traded via internet sites. In addition, misuse of data on the internet harms the rights of others, and personal data is part of human rights that must be protected.

The existence of a vulnerability in the e-commerce cyber security system in Indonesia related to personal data leakage requires the Government to have a legal solution to this issue. Because of this, the Government and the DPR RI recently agreed to pass Law No. 27 of 2022 concerning Personal Data Protection as a legal regulator for issues of personal data leakage. This legal regulator is an effort by the Government of the Republic of Indonesia to provide guarantees and legal protection to every citizen who uses e-commerce. Because of this phenomenon, this study aims to evaluate the protection of personal data in transactions using e-commerce from the perspective of Indonesian law.

II. METHODS

A. Research Approach

This study uses a normative legal evaluation approach and normative-empirical law [6].

1) Normative Legal Approach

Normative legal research used in this research is by researching and examining literature or library materials. This approach uses secondary data.

2) Normative Legal Approach – empirical

Normative-empirical legal research in this study evaluates the implementation of normative legal provisions (laws) that occur in a society.

This study uses a statutory approach (statute approach) which reviews legislation based on primary legal materials, a Comparative Approach, and a Conceptual Approach based on secondary and tertiary legal materials [7],[8].

B. Data Type

This research uses some legal data to evaluate which consists of primary, secondary, and tertiary legal materials [9], namely:

Table I. Research Data

No	Law Data	Data type
1	Primary Legal Materials	Article 28 G paragraph (1) of the 1945 Constitution Law Number 27 of 2022 concerning the Protection of Personal Data Law Number 8 of 1999 concerning Consumer Protection; Law No. 7 of 2014 concerning Trade Law Number 39 of 1999 concerning Human Rights; Law Number 23 of 2006 concerning Population Administration as amended by Law Number 24 of 2013 Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016. Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Government Regulation No. 80 of 2019 concerning Trading Through Electronic Systems. Minister of Communication and Informatics Regulation No. 20 of 2016 concerning the Protection of Personal Data in Electronic Systems
2	Secondary Legal Materials	Books or legal literature on Personal Data, e-commerce, Online Transactions, Consumer Protection and Public Information Disclosure. Dissertations, theses, and legal thesis related to the object of research International Journals, Accredited or non-accredited National Journals. Working Papers on important conferences, scientific seminars, scientific symposiums
3	Tertiary Legal Materials	Legal materials to support Primary Legal Materials and Secondary Legal Materials, such as: abstracts, official government publications, official minutes, scientific magazines, documents, dictionaries, websites, and others.

C. Data Analysis

This study uses a normative legal approach by reading descriptive data in the form of descriptions and verbal information stated by respondents in writing or verbally from actual behavior. The analytical technique is qualitative analysis to study human life in limited cases, casuistic in nature, but more in-depth [10].

III. RESULTS AND DISCUSSION

A. Legal protection for personal data protection in the Consumer-to-Consumer concept of using online transactions based on applicable laws and regulations

1) 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 country.

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 that 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.

2) 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 marketplace online.

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 e-commerce activities.
c) The creation of 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 strategy is a form of benefit 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. Preventive/cautionary measures are needed from consumers to include their private data because when the company processes consumers' data, then there are rights violated by consumer privacy. So far, there have been forms of public complaints reported to the e-business directorate, the Ministry of Communication and Informatics, mainly 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.

B. Personal Data Protection Regulations

Using personal data in e-commerce transactions is necessary to verify data on personal 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 very bad problems due to the inconvenience caused to someone who has leaked the personal data.

There is a risk that occurs when personal data is leaked and used by irresponsible people, so they tend to commit crimes in utilizing personal data, including First, personal data can be used to break into financial accounts. This problem is done using social manipulation by tricking the victim. For example, perpetrators can send emails 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 real data owner doesn't even know about the lending problem, so he gets bad 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 of social media accounts 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, so 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.

C. 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 Law - 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 according to 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, ensuring 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.

D. Data Protection Guarantee in E-commerce Transactions

The article explains that the trustee 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. Then, if the 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 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 the Protection of 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.

Thus, 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 conducting 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.

E. 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 the use of online transactions is increasingly developing and advanced, requiring other countries to have regulations to ensure the security of their citizens' personal data. Several rules in several countries have become a reference for the making of Law No. 27 of 2022 concerning Personal Data Protection in Indonesia

Table II. Protection of Personal Data in Some 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 [11]. In developing the latest legal provisions regarding data protection in the European Union, namely EU

No	Country	Information
		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) [12]. 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 [13].
2	United States of America	Based on the US Privacy Act 1974, the United States Department of Health in 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 [14]. 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.

F. Settlement of Personal Data Protection Disputes

Legal guarantees, protection, and certainty cannot be fulfilled without institutional authority. Thus, 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 committed by e-commerce parties, whether intentional or unintentional.

IV. 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 for 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 personal data protection 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 within approximately 2 years, so this law will be optimally effective for only 2 years to come. After the promulgation of Law No. 27 of 2022 concerning the Protection of Personal Data, only administrative sanctions can be imposed if personal data is misused in e-commerce. 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.

Personal data protection regulations are still partial to date, so Law No. 27 of 2022 concerning Protection of Personal Data does not yet have maximum legal force purely as a legal umbrella for personal data security from data leakage by third parties. Because of this weakness, other legal remedies are needed to support Law No. 27, namely 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 Protection of Personal Data in Electronic Systems as a legal umbrella for guaranteeing the security of personal data protection.

The guarantee of security for personal data protection in Indonesia is still not optimal because the implementation of regulations on guarantees for personal data protection is still not optimal. After all, these regulations are still partial so other legal remedies are still needed in dealing with the problem of the leakage of personal data in Indonesia. The current Government has not made derivative regulations as 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 that these business actors are also part of the collection and processing of consumers' personal data in conducting online transactions activities. So, compliance with the online marketplace must follow the Government Regulation to ensure the continuity of personal data security for each consumer in buying and selling transactions. However, the problem with Government Regulation No. 80 of 2019 concerning Trading Through

Electronic Systems is that Government Regulation No. 80 does not specifically stipulate criminal sanctions to be imposed. Government Regulation no. 80 is only limited to regulating administrative sanctions so that problems with personal data leakage cannot be resolved optimally if data leakage cases recur and impact consumer convenience in conducting online buying and selling transactions at online marketplaces.

REFERENCES

[1] Zou H. Protection of personal information security in the age of big data. Proc - 12th Int Conf Comput Intell Secur CIS 2016. 2017;586–9.

[2] Wu Y. Protecting personal data in E-government: A cross-country study. Gov Inf Q. 2014;31(1):150–9.

[3] Kominfo. Pasal 1 angka 1 Peraturan Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. 2016.

[4] Kominfo. Pasal 1 angka 2 Peraturan Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik. 2016.

[5] Malia I. Sebelum BPJS Kesehatan, Ini 3 Kasus Kebocoran Data Konsumen E-commerce. IDN times. 2021;

[6] Mukhti Fajar, Achmad Y. Dualisme Penelitian Hukum Normatif dan Empiris. 2015;8(1):15–35.

[7] Rakhmawati NA, Rachmawati AA, Perwiradewa A, Handoko BT, Pahlawan MR, Rahmawati R, et al. Konsep Perlindungan Hukum Atas Kasus Pelanggaran Privasi Dengan Pendekatan Perundang-Undangan Dan Pendekatan Konseptual. Justitia J Huk Fak Huk Univ Muhammadiyah Surabaya. 2019;3(2):297–304.

[8] Kaimudin A. Perlindungan Hukum Terhadap Tenaga Kerja Anak Dalam Perundang- Undang Di Indonesia. Yurispruden. 2019;2(1):37.

[9] Mangku DGS, Radiasta IK. Tanggung Jawab Negara terhadap Penembakan Pesawat MH17 berdasarkan Hukum Internasional. Pandecta Res Law J. 2019;14(1):25–33.

[10] Putra RDW, Indradjati RPN. Studi Deskriptif – Evaluatif Bentuk Tipologi Kawasan (Pembelajaran Dari Kota Surabaya). J Pengemb Kota [Internet]. 2021 Dec 28;9(2):124–42. Available from: https://ejournal2.undip.ac.id/index.php/jpk/article/view/9827

[11] Makarim E. Pengantar Hukum Telematika : Suatu Kompilasi Kajian. Jakarta : Raja Grafindo; 2005. 150 p.

[12] Tsamara N. Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. J Suara Huk. 2021;3(1):60.

[13] Ramadhani SA. Komparasi Pengaturan Perlindungan Data Pribadi di Indonesia dan Uni Eropa. J Huk Lex Gen. 2021;3(21):78.

[14] 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.