Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia

Tegar Islami Putra¹, Nurul Fibrianti²

¹Faculty of Law, Semarang State University
Sekaran Raya Street, Gunung Pati District, Semarang City, Central Java
tegarislami44@students.unnes.ac.id
²Faculty of Law, Semarang State University
Sekaran Raya Street, Gunung Pati District, Semarang City, Central Java
nurulfibrianti@mail.unnes.ac.id

Submitted : 18/01/2024 Reviewed: 14/03/2024 Accepted: 30/03/2024

Abstract: The dynamics of Indonesian trade are becoming more complex as time goes on, and one form of this development is digitalization. Although it has a positive impact, trade digitization also has a negative impact on different points of view, one of which is the threat in terms of combined personal data. Combined personal data is one type of personal data that is protected by the state through legal protection, so that the state guarantees people’s personal data. This scientific research uses one part of the grand method, namely Library Research which is based on literature or literature. The results of the research show that there are three forms of threats to people’s personal data combined in e-commerce transactions, especially in the use of IP Address, namely threats to geographic location tracking, unauthorized use and opening of personal data, and Distributed Denial of Service (DDoS) attacks. In the legal space in Indonesia, the three threats themselves do not yet have further rules related to the form and mechanism of protection and have different arrangements as a form of protection. Law Number 27 of 2023 concerning Personal Data Protection, Law Number 19 of 2016 amending Law Number 11 of 2008 concerning Electronic Information and Transactions, and Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions. Based on this research, it is necessary to provide legal rules related to the form and mechanism of protecting a person’s IP Address as one type of personal data in Indonesia.

Keywords: Threats; Legal Protection; Consumer; Personal Data; E-Commerce

DOI: 10.32801/lamlaj.v9i1.438

INTRODUCTION
Humans are creatures that need the presence of other people in their lives, because humans are social creatures who cannot live their lives alone.¹ Humans as social creatures always need the help of others in their daily lives, including in carrying out economic activities. Economic activities such as buying and selling, renting, and making loans.² Humans basically always try their best to achieve efficiency and effectiveness in

every action they take. In this case, buying and selling transactions are no exception. Various kinds of online service facilities available in the community to facilitate buying and selling activities, ranging from online payment facilities, online shopping, to online transportation can easily be enjoyed through e-commerce facilities that are widely available today. The presence of accurate and efficient e-commerce can reduce the risk of unwanted errors and increase the efficiency of selling products or services. In today’s digital era, buying and selling goods online is increasingly popular in Indonesia. Various e-commerce platforms have mushroomed, allowing consumers to purchase goods easily without the need to visit a physical store.

According to Bank Indonesia data, digital transactions in 2020 amounted to IDR 27.4 trillion and continued to increase to IDR 40 trillion in 2021, and is expected to continue to increase to IDR 48.6 trillion in 2022. Based on Statista Market Insights data, the number of online marketplace or e-commerce users in Indonesia will reach 178.94 million people by 2022. This number increased by 12.79% compared to the previous year which amounted to 158.65 million users. This number continues to increase, given the benefits of increased business competence, higher labor efficiency, global transactions, offering customers a wider and more diverse product range, and business growth. The prevalence of data breach breaches, both domestically in Indonesia and international underscores the critical importance of integrating robust data protection measures into existing legal frameworks. The official website of the Ministry of Communication and Information of the Republic of Indonesia states that in a study entitled eConomy SEA 2022, the value of Indonesia’s digital economy is predicted to reach USD 77 billion by 2022. This figure reflects a 22 percent growth on an annual basis. Of this total, Indonesia’s e-commerce contribution contributed USD 59 billion and is expected to reach IDR 33.06 trillion by 2022.

---


to increase to USD 95 billion by 2025. The ease of access to do business online, the wide reach, and the large number of internet users in Indonesia encourage people to open a stall to make a profit.\(^{11}\) However, these positive impacts and advancements have also led to new problems, including the easy collection and transfer of an individual’s personal data without the knowledge and consent of the data subject. This threatens the constitutional rights of personal data subjects and emphasizes the importance of personal data protection in response to such challenges.\(^{12}\) In terms of personal data protection in Indonesia alone, no less than 466 million personal data were allegedly leaked after the enactment of the Personal Data Protection Law.\(^{13}\) In addition, on April 17, 2020, e-commerce Tokopedia experienced a leak of its users’ personal data, at least for 12,115,583 accounts.\(^{14}\) So in this case it is considered important to give further attention to personal data. According to Zheng Qin in his book Introduction to E-Commerce,\(^{11}\) when conducting and accepting online transactions, it is necessary to provide consumers’ personal data.

In response to this, the government did not remain silent. Since 2019, Law (UU) Number 27 of 2022 on Personal Data Protection was approved and passed. This ratification coincides with the rise of many leaks of personal data. In its consideration, this regulation has the function of guaranteeing citizens’ rights to personal protection and ensuring recognition and respect for the protection of personal data.\(^{16}\) As stipulated in Article 4 paragraph (1), this Law divides personal data into two parts, namely specific personal data and general personal data. The specific personal data includes health data and information, biometric data, genetic data, criminal records, child data, personal financial data; and/or other data in accordance with the provisions of laws and regulations.\(^{17}\) Furthermore, general personal data as stipulated in the PDP Law is data that includes name, gender, nationality, religion, marital status, and/or personal data combined for individual identification.\(^{18}\)

Article 1 point 1 of Law No. 27 of 2022 provides the nomenclature of personal data


\(^{18}\)Ibid.
as data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems.\textsuperscript{19} In the explanation of Article 4 paragraph (3) letter f, it states that IP (Internet Protocol) Address and cellular phone number are personal data combined to identify a person and are general Personal Data. IP Address is a series of numbers that represent the identity of a device when connected to the internet or other network infrastructure.\textsuperscript{20} This IP Address is definitely utilized in e-commerce, considering that e-commerce is a platform that utilizes the internet. While the phone number is used to support the effectiveness of the use of cellular phones, namely the connection of services from telecommunications service providers that require the activation of a Subscriber Identification Module Card (SIM Card) or telephone number.\textsuperscript{21}

However, IP Address and cellular phone number as general personal data themselves do not have further regulations related to the form and mechanism of protection. In addition, IP Address is something that is rarely heard and known by the general public, so they do not understand and know more about the threats to the IP Address. Based on this, it is important to be protected, especially in terms of e-commerce implementation related to threats to IP Addresses and telephone numbers as a form of personal data combined. Therefore, this paper aims to analyze the threats of consumer personal data combined in e-commerce transactions and to analyze the form of protection of personal data combined in e-commerce transactions based on personal data protection laws.

Based on the explanation above, this paper aims to find the form of threats to consumer personal data combined in e-commerce transactions and identify the form of protection for consumer personal data combined in e-commerce transactions in Indonesia.

METHOD

Scientific research uses one of the grand method sections, namely Library Research which is based on literature. Based on the subject of study and the type of problem, of the 3 (three) types of grand methods mentioned above, this research will use the Library Research method. Regarding this kind of research, it is also commonly called “Legal Research”.\textsuperscript{22} This kind of legal research does not recognize field research (field research) because what is studied is legal material so that it can be said to be library based, focusing on reading and analysis and analysis of the primary and secondary materials.\textsuperscript{23}

Research Sites

This research utilizes the Social Science Research Network (SSRN) website to access and analyze academic articles and journals in


\textsuperscript{22} Soerjono Soekanto and Sri Mamudji, \textit{Penelitian Hukum Normatif Tinjauan Singkat} (Jakarta: Rajawali Press, 2006): 36

order to review existing literature. Additionally, the research makes use of the Directory of Supreme Court Decisions of the Republic of Indonesia to obtain relevant court rulings.

ANALYSIS AND DISCUSSION

Threats of Personal Data Combined in E-Commerce Transactions

The concept of data protection and cyber security is a form of effort made to protect user identity from various threats and illegal access. In general, in the cyber world, cyber threats can be access by unauthorized people to access data and misuse personal information, facilitate attacks on other systems, and threaten the personal safety of users.

In the current era of the Industrial Revolution 4.0, digitalization has penetrated into the realm of privacy. E-Commerce media platforms must be able to provide security and protection of personal data that can provide a sense of security, and comfort in the buying and selling process and conform to the Personal Data Protection Law.

Indonesia ranked third with the highest number of accounts that experienced data breaches in the third quarter of 2022. With more than 12 million hacked accounts and cases increasing every month. This number is a collection of data from several threats. Regarding personal data that is combined as described in Article 4 paragraph (3) letter f of the Personal Data Protection Law, the explanation of the paragraph explains that personal data combined to identify a person includes IP Address and cell phone number.

The first combined personal data-related threat is geo-location tracking by irresponsible parties by utilizing a person’s IP Address. An IP address can show geolocation in the form of a city and even a person’s address. Based on the IP Address, information can be obtained to track the location of the user. This number is a collection of data from several threats. Regarding personal data that is combined as described in Article 4 paragraph (3) letter f of the Personal Data Protection Law, the explanation of the paragraph explains that personal data combined to identify a person includes IP Address and cell phone number.

The first combined personal data-related threat is geo-location tracking by irresponsible parties by utilizing a person’s IP address.


27 Ibid.


An IP address can show geolocation in the form of a city and even a person’s address. Based on the IP Address, information can be obtained to track the location of the user.

The second combined personal data-related threat is the unauthorized use and disclosure of personal data. If someone knows the victim’s IP address, they can try to connect to the victim’s device. The hacked IP address may reveal the identity of the Country, State or region, City, Internet service provider (Approx), GPS coordinates, and IP address type (private, static, dynamic, or public IP address).

In addition, there is a leak of traceable application user data. Sensitive customer data such as name, coordinates, phone number, address, and destination can still be accessed through the API endpoint. Another thing that can be utilized by hackers against a person’s IP Address is knowing a person’s Digital Trace, which is knowing a person’s digital record of what digital activities in cyberspace. This is a form of Cyber Espionage which is a crime that utilizes the internet network to conduct spying activities on other parties, by entering the target party’s computer network system. Sabotage and Extortion are crimes committed by disrupting, damaging or destroying data, computer programs or computer network systems connected to the internet.

The third combined personal data-related threat is a Distributed Denial of Service (DDoS) attack. DDoS attacks can impair network or website performance by sending extremely high internet traffic to a target IP Address. If your IP Address is not protected, you are vulnerable to such attacks. In a DDoS attack, the attacker uses thousands or even millions of connected devices to achieve his goal, thus making it more difficult to defend against. Affected services may include email, websites, online accounts (for example, banking), or other services that rely on the affected computer or network. Denial-of-service conditions are performed by flooding the targeted host or network with traffic until the target is unable to respond or crashes, preventing access for legitimate users.

Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia

Referring to the 2009 Madrid Resolution, personal data protection regulations must regulate enforcement mechanisms, at least some of which are capable of being applied to

---

36 Ibid.
37 Ibid.
provide sanctions varying from mild to very high. Then, the need for proactive and systemic enforcement actions, with the existence of an independent data protection authority.\textsuperscript{40}

Today, the world has entered the Zettabyte era, where global IP (Internet Protocol) based communication traffic has increased rapidly in the past three years.\textsuperscript{41} The IP Address in global traffic itself cannot be underestimated. Law No. 27 of 2022 even makes IP Address an object of personal data that needs to be given protection. Against a person’s IP Address as previously explained, that there are several threats to a person’s IP Address, where the IP Address can be used as a medium for tracking a person’s geographic location, wiretapping or unauthorized use and opening of personal data, and DDoS attack media. So it is important to be given protection.

Indonesia is a country based on law in accordance with Article 1 paragraph 3 of the 1945 Constitution. This makes the law the commander-in-chief that binds the lives of Indonesian people. Law is needed to provide protection, justice and certainty.\textsuperscript{42}

Regarding a person’s IP Address as public personal data as mandated by Article 4 paragraph (3) letter f of Law No. 27 of 2022, the protection of the first threat that needs to be considered is the use of IP Address as a means of geographic tracking of a person. In Law Number 27 of 2022, this contradicts the principles of protection and confidentiality as mandated by Article 3 letters a and h. This law does not explain more deeply the protection of a person’s geographical tracking.

However, the geo-tracking of a person is related to the mandate in a different law, namely in the explanation of Article 26 paragraph (1) of Law Number 19 Year 2016 which amends Law Number 11 Year 2008. In the explanation of this paragraph, it reads:

“In the use of Information Technology, personal data protection is one part of personal rights: (c) Personal rights are the right to control access to information about one’s personal life and data.”

As a follow-up to this paragraph, Article 26 Paragraph (2) explains that:

“Any person whose rights are violated as referred to in paragraph (1) may file a lawsuit for the losses incurred under this Law.”

The second threat protection that needs to be considered is the use of IP Address for wiretapping by irresponsible people. Although Law No. 27 of 2022 makes IP Address as one of the types of personal data, this law does not explain further regarding the act of utilizing one’s IP Address for wiretapping.

However, the use of a person’s IP Address for wiretapping is regulated under different rules. This is regulated in Law Number 19 Year 2016. In this case, it is explained in Article 30 paragraph (1) which reads:

“Every Person intentionally and without right or unlawfully accesses another Person’s Computer and/or Electronic System by any means whatsoever.”

In this regard, if there is a violation of Article 30 paragraph (1), then Article 36 of Law Number 1 of 2024 as an amendment to Law Number 19 of 2016 applies, which reads:

“Every Person intentionally and without right commits acts as referred to in Articles 30 through 34 which result in mate-
In this case, the rules in Article 51 of Law Number 1 Year 2024 as an amendment to Law Number 19 Year 2016 also apply, which reads:

“Every person who fulfills the elements as referred to in Article 36 shall be punished with a maximum imprisonment of 12 (twelve) years and/or a maximum fine of Rp12,000,000,000.00 (twelve billion rupiah).”

The third threat protection that needs to be considered is the use of IP Address for DDoS attacks. Although Law No. 27 of 2022 makes IP Address as one of the types of personal data, this law has not explained further regarding the act of utilizing one’s IP Address for DDoS attacks.

Law No. 27 of 2022 does not provide explicit protection against DDoS attacks, but the utilization of a person’s IP Address for DDoS attacks can be subject to other clauses with fulfilled elements related to losses obtained by victims and applicable laws and regulations.

Even though there are several rules above, the violations above still refer to Article 15 paragraph (2) letter b of Law Number 11 of 2008 which reads:

“Electronic System Operator is responsible for the implementation of its Electronic System.”

So that in this case, every electronic organizer is still responsible for the electronic implementation that he does. However, it should be noted that Article 15 paragraph (2) does not apply in the event that it can be proven that force majeure, error, and/or negligence of the Electronic System user as regulated in paragraph (3).

In addition, it should be noted that Article 4 letter b of Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, explains that:

“Every Electronic System Operator must operate an Electronic System that meets the minimum requirements to protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the implementation of the Electronic System.”

Based on these rules, it can be understood that electronic system providers are required to meet these minimum requirements to protect personal data and other important information collected from their users. In the event of a violation of this, the electronic system organizer can be given administrative sanctions as stipulated in Article 100 paragraph (1). Article 100 paragraph (2) then explains that the administrative sanctions can be in the form of a written warning, administrative fines, temporary suspension, termination of access; and/or excluded from the electronic system registration granted by the minister. In this case, it is necessary to provide legal rules related to the form and mechanism of protecting a person’s IP Address as one type of personal data in Indonesia.

CONCLUSION

Based on the results of the analysis, it can be concluded that there are two types of personal data combined based on the rules applicable in Indonesia, namely IP Address and telephone number. This IP Address is definitely utilized in e-commerce as a platform that utilizes the IP address. The form of threat to this IP Address is that it can be used to track geographic location, unauthorized use & opening of personal data, and Distributed Denial of Service attacks. In the legal space
in Indonesia, the protection provided for these threats is not only regulated in Law Number 27 of 2023 concerning Personal Data Protection, but also regulated in Law Number 19 of 2016 which amends Law Number 11 of 2008 concerning Electronic Information and Transactions, and Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

BIBLIOGRAPHY

Books


Journal


Putra, Tegar Islami, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman. “Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical


Internet