



Protecting Digital Dignitas: Highlighting Legal Protection and Responsibility in Personal Data Security Crime in Indonesia's Online Marketplace World

Dinda Yunisa^{1*}, Adelina Mariani Sihombing², Chelsea Mutiara Putri³, Nurul Hasanah⁴

^{1,2,3} Universitas Sumatera Utara, ⁴ Asia E University

*Correspondence Email: dindayun86921@gmail.com



Abstract:

Today the development of technology is increasingly massive and gave birth to a form of intelligence called *Artificial Intelligence/AI*. Economic potential and threats of personal data leakage awaiting immediate investigation. The concept of digital dignity is closely related to personal data security because in the digital era, leakage of personal data can harm users and violate their privacy rights. This paper aims to provide a juridical analysis of digital identity protection by highlighting legal protection and marketplace responsibility for cases of personal data leakage in Indonesia. The type of research used is normative legal research using statutory regulations, case studies and concept approaches. This research uses secondary data as the main data and uses literature study as a material collection technique. All materials that have been collected are then inventoried, classified, and analyzed using descriptive analysis which aims to describe the problem so that innovative solutions are obtained. There are several deficiencies in the marketplace security system and regulations governing the protection of personal data. This can be handled with marketplace supervisory agencies or supervisory parties, implementing standardized security and regulations on marketplaces specifically as well as internal and external digital identity protection regarding the several parties involved in it.

Keywords: : Marketplace, Digital, Personal data protection

INTRODUCTION

Today the development of the world of technology is increasingly massive in various parts of the world, including Indonesia. Various progress occurred significantly and could not be stopped. One of the implications of this technological advancement is the birth of Artificial Intelligence (AI). AI, which usually helps human work, is referred to as a smart invention, like gold in the history of human technological development. The discovery that originated from the concept that machines are believed to be capable of processing information and solving problems stems from Alan Turing in 1947 which has provided a major differentiation in people's lives.¹Then over time, now AI has touched various sectors or areas of life such as banking, communications, land security, industry, transportation, health, education and the economy.

In the economic field, AI can take the form of machine learning technology, using algorithms that can analyze files or economic data on a large and large scale, but the speed exceeds that of humans.²In another form, namely in the form of developments in the world of

¹ Reni Susanti, Artificial Intelligence: Definition, How it Works, Development and Impact, accessed on Saturday, 27 May 2023 at 20.22 WIB., via Artificial Intelligence (AI): Definition, Development, How It Works, and Its Impact (kompas.com).

² Medan Area University Admin, The Role of AI in the World Economy, accessed on Saturday, 27 May 2023 at 20.30 WIB via The Role of AI in the World Economy - (uma.ac.id).

economic activity transactions such as buying and selling which are carried out virtually through electronic markets known as marketplaces. Marketplaces are proven to be popular with Indonesians based on a report from AppsFlyer, an application tracking company with the title "The state of e-commerce app marketing 2021" stating that Indonesia is the third country in the world that uses the most marketplaces.³ Furthermore, according to data from the Central Statistics Agency, marketplace users continue to increase from year to year, especially from 2020 and above by as much as 70% increase from 15,677 business samples in all Indonesian provinces.⁴ As we know, Indonesia's digital economy is currently experiencing rapid development. According to the 2021 World Bank report, Indonesia is among the top five countries in the world with the highest level of internet usage. On average, eighty percent of Indonesian people's time is used to utilize internet technology both for communicating, surfing social media, and doing business.⁵

Reflecting on the very large number of marketplace users in Indonesia, this gives us an illustration that this is a double-edged sword, a potential as well as a threat if not further analyzed. The acceleration of significant marketplace developments as a result of the progress of AI will have negative consequences if it is not followed up by regulations and upholds integrity, values of rights, ethics and legal protection and responsibility. For example, as in the case that occurred recently, namely the leakage of consumer personal data which is the realm of privacy. If this case is increasingly mushrooming in society, then how many people will lose out due to fraud or other crimes. The public's memory is still wet with cases that occurred in 2020 ago, namely the leakage of personal data of one point two million Bhinneka.com users and being traded on the dark web. Another case occurred in the Tokopedia marketplace where 91 user data and seven million seller data were allegedly leaked in May 3 years ago. Then as many as thirteen million Bukalapak user account data were also hacked in 2019.⁶ Of course it is detrimental to society and the marketplace.

As a result the cases that occurred in Indonesia have violated the law itself. This refers to the concept of digital identity protection as a concept that is oriented towards self-esteem, integrity and individual rights in a digital environment such as a marketplace. This includes recognition and protection of privacy, security of personal data and freedom to interact and participate in the digital world. Digital Dignitas emphasizes the importance of respecting and protecting individual dignity in the context of technology and online communication. In this case, it is necessary to have legal and regulatory protection as a form of responsibility from related parties. This scientific paper will examine how the marketplace security system actually works.

Based on the background above, the formulation of the problem in this scientific work is as follows:

1. How is the security of the personal data of consumers who use the marketplace in Indonesia?
2. How is the legal protection of the personal data of consumers who use the marketplace in Indonesia?
3. What is the role of law in marketplace accountability for data leak cases in Indonesia in the concept of digital dignity?

³ Galuh Putri Riyanto, Third Largest Number of Marketplace Application Users in the World, accessed on Saturday, 27 May 2023 at 20.37 WIB., via Indonesia's Third Largest Number of Marketplace Application Users in the World Page all - Kompas.com.

⁴ Central Bureau of Statistics, Central Bureau of Statistics (bps.go.id)

⁵ Firman Hidranto, Encouraging G20 Sustainable Digital Transformation, accessed on Saturday, May 27 2023 at 21.00 WIB. -g20?lang=1

⁶ Reni Susanti, Rows of Personal Data Leakage Cases in the Last Two Years, accessed on Sunday, May 28 2023 at 09.00 WIB., via Rows of Personal Data Leakage Cases in the Last Two Years... (kompas.com).

METHOD

The type of research used in the writing of this study is normative legal research or library law research, namely research conducted by examining library materials or mere secondary data.⁷ Therefore, the main data source used is a secondary data source. Approach is one way to approach the object of research. Approaches that are commonly used in legal research are statutory approaches. Approaches that are commonly used in legal research are statutory approaches, case approaches, historical approaches), a comparative approach (comparative approach), and a conceptual approach (conceptual approach).⁸ The approach used in this study is a statute approach and a conceptual approach. The legal material collection technique used in this research is literature or document studies. Literature or document study is an activity of collecting and examining or tracing documents or literature that can provide information or information needed by researchers.⁹ This means that the collection of materials is done by means of library data (library research), identifying laws and regulations, researching library materials, reading books and other sources related to environmental crimes.

ANALYSIS AND DISCUSSION

Security of the Consumer Personal Data System for Online Marketplace Users in Indonesia

Along with the development of the times, the use of technology continues to grow rapidly, one of which is in the field of trade. Today's trading is not only done face-to-face (conventionally) but has now been implemented through virtual space (cyberspace). Trading through virtual is known as e-commerce where consumers can make buying and selling transactions using only the internet wherever and whenever. Activities in e-commerce can be carried out through various platforms, namely marketplaces, social media and websites. One platform that has become a trend since 2020 is a marketplace such as Tokopedia, Shopee, Bukalapak, Lazada, Bhinneka and other online shopping platforms. Apart from being an online shopping trend,¹⁰

In Indonesia alone, based on data released by Bank Indonesia in September 2020, e-commerce transactions in Indonesia have a transaction value of up to IDR 180.74 trillion.¹¹ This value certainly shows that e-commerce is very popular in Indonesia. The presence of e-commerce does make it easy for consumers to shop. But on the other hand the use of e-commerce does not always have a positive impact but can also cause problems that have a negative impact. One of the main problems that often arises is the leakage of consumer personal data. In practice, online marketplace users are required to register first by filling in a number of personal data on the platform. The receipt of personal data by the online marketplace triggers the vulnerability of data leakage which will cause harm to consumers.

Basically, the security system in e-commerce includes several important aspects that are used as a basis, namely basic security aspects consisting of security aspects, various threats, and solutions to deficiencies in e-commerce systems. All these important aspects of e-commerce are very influential on the level of security of e-commerce as a whole.¹² There are two main things that must be considered in making transactions related to transaction security and the methods used to create this security. The dimensions of security in E-commerce are:¹³

⁷ Soerjono Soekanto., and Sri Mamudji, Normative Legal Research; A Brief Overview, PT. Raja Grafindo Persada, Jakarta, 2003, p.13.

⁸ M. Syamsudin, Legal Research Operations, Rajawali Press, Jakarta, 2007, p. 56-57

⁹ Ibid, p.101.

¹⁰ SIRCLO, "Number of Indonesian E-Commerce Users in 2020 Increases Rapidly" can be accessed at <https://www.sirclo.com/blog/nomor-user-e-commerce-indonesia-di-tahun-2020-meningkat-pesat> accessed on 21 May 2023

¹¹ CNN Indonesia, "E-Commerce Transactions Reach IDR 180.74 T as of September 2020" can be accessed on <https://www.cnnindonesia.com/economy/20201215150353-78-582406/transaksi-e-commerce-reach-rp18074-t-per-september-2020> accessed on May 21, 2023

¹² I Gusti Ngurah Indra Saputra, et al. 2017. "Development of Security Systems for E-Commerce." PIGEON VOL 5 NO 1 17.

¹³ Andre MR Wajong and Carolina Rizky Putri. 2010. "Security in Electronic Commerce." ComTech Vol 1 No 2 20.

1. Authentication, the identity of the buyer, seller, and payment institution involved must be ensured as the party entitled to be involved in the transaction
2. Integrity, assurance that the data and information transferred to e-commerce remains intact and does not change
3. Non-repudiation, the customer needs protection against denial from the seller that the goods have been delivered or payment has not been made. Information is needed to determine who the sender and recipient are.
4. Privacy, customers want their identity to keep their data safe.
5. Safety, customers want assurance that it is safe to provide internet credit card number information

Furthermore, in order to provide guarantees for the protection of personal data, besides the need to improve system security, regulatory arrangements are also needed as a legal umbrella for the protection of consumer personal data, especially in Indonesia. regulations governing these activities are among others contained in Law Number 7 of 2014 concerning Trade, Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE) which is an amendment to Law No.11 of 2008 and Law Number 8 of 1999 on Consumer Protection, as well as the latest regulations regarding E-Commerce is Government Regulation Number 28 of 2012 concerning Implementation of Electronic Systems and Transactions.¹⁴

Tokopedia

Tokopedia as an online marketplace in Indonesia is committed to protecting the privacy policies of its users. However, there are several privacy policies from Tokopedia that have the potential to threaten the security of its user data, such as the user data acquisition and collection system where transaction activities are carried out through various sites such as bank account data, credit cards, virtual accounts, instant payments, internet banking, and retail outlets. . With a wide and unlimited coverage of payment data, it has the potential to cause a breach of a user's bank account. Data recorded when a user uses the site, including but not limited to real or approximate location data such as IP address, Wi-Fi location, geo-location will greatly allow the data to be leaked and misused. Furthermore, Tokopedia can combine data obtained from other sources with other data. The fact is that this data is not specifically explained regarding the mechanism and type of data that is combined so that it will trigger problematic data. Moreover, this is not in line with what is stated in article 599 paragraph (2) letter b PP PMSE which states that personal data must be owned only for one purpose that has been specifically and legally described. The data is prohibited from being processed further in a way that is inconsistent with that purpose. The fact is that this data is not specifically explained regarding the mechanism and type of data that is combined so that it will trigger problematic data. Moreover, this is not in line with what is stated in article 599 paragraph (2) letter b PP PMSE which states that personal data must be owned only for one purpose that has been specifically and legally described. The data is prohibited from being processed further in a way that is inconsistent with that purpose. The fact is that this data is not specifically explained regarding the mechanism and type of data that is combined so that it will trigger problematic data. Moreover, this is not in line with what is stated in article 599 paragraph (2) letter b PP PMSE which states that personal data must be owned only for one purpose that has been specifically and legally described. The data is prohibited from being processed further in a way that is inconsistent with that purpose.

Bukalapak

Bukalapak's privacy policy contains the phrase "unrestricted", one of which can be found in policies related to data acquisition and protection which states that Bukalapak has the right to request user data and information including the behavior of Bukalapak users and/or while using information services on product choices, features and services. , as well as other user information which includes but is not limited to registration, login, transaction activities and others. In this case, other information associated with the phrase "unlimited" becomes very vague so that users do not know the extent of the data accessed and the consequences that may arise in the future.

¹⁴ Maichel Delpiro, et al. 2021. "Juridical Analysis of Privacy Policy and Online Market Place Accountability in the Protection of Users' Personal Data in Cases of Data Leakage." *Padjadjaran Law Review* Vol 9 No 1 32.

Bhinneka

As with other online market places previously described, the establishment of a privacy policy for Bhinneka also has weaknesses, especially related to compensation which states that Bhinneka is not responsible for user losses caused by actions against hacking personal data on user accounts. This shows that this policy can be said as a form of full release of responsibility from Bhinneka as an online marketplace that obtains, collects and processes user data.

The weakness of the online marketplace policy is actually not in line with the Basic Principles of National Application OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, there are two principles that must be met, namely:¹⁵

1) *Collection Limitation Principle*(Principle of Collection Restriction)

It is a principle which states that there are limitations in the collection of personal data and the like which are obtained through lawful and fair means, and in accordance with the consent of the data subject. If you look at the policies of the three online marketplaces above which contain the phrase "unlimited" especially in data acquisition and collection and do not provide specific explanations regarding the use of data so that they are not in accordance with this principle.

2) *Security Safeguards Principle*(Principle of Security Protection)

Which states that data must be protected with appropriate security safeguards to avoid risks such as loss of unauthorized access, destruction, use, modification or disclosure of data. Tokopedia's policy of not being able to provide 100% protection until Bhinneka's hand is released for compensation for hacking actions can be found not to provide protection and safeguards for user data security.

Legal Protection of Marketplace Users' Personal Data in Indonesia

It is stated in the fourth paragraph of the Preamble of the 1945 Constitution, stating that the Indonesian government is constitutionally obliged to provide protection for citizens and improve general welfare, educate the nation's life, and be involved in world order based on freedom, eternal peace, and social justice. In the context of technological development, the state has a goal in the form of protecting the personal data of each citizen. In general, it is acceptable if the 1945 Constitution as a constitution provides a policy for tackling acts of stealing personal data by protecting personal ownership of all parties trying to break into or steal data belonging to other parties.¹⁶

Protection of personal data has been regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), which is stated in Article 26 Paragraphs (1) and (2) which states that:¹⁷

1. Unless otherwise stipulated by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned.
2. Every person whose rights are violated as referred to in Paragraph (1) can file a claim for losses incurred under this law.

The provisions regulated have given the right to the owner of the personal data to maintain the confidentiality of his personal data. If his personal data is spread and can be misused by other parties, the owner of the personal data can file a lawsuit in court. The lawsuit in question is in the form of a civil lawsuit filed based on statutory regulations.¹⁸The provisions of this article constitute protection given to a person's personal data in general, meaning that in any activity involving electronic transactions that use a person's personal data it is mandatory to safeguard and protect that personal data. Any personal data that has been provided must be used in accordance with the consent of the person who has it and must be kept confidential.¹⁹

Consumers who feel aggrieved due to leakage of personal data in online transactions on the

¹⁵ Refer to the Basic Principles of National Application OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Part Two Basic Principles of National Application

¹⁶ Natha, KDR, Budiarta, NP, & Astiti, NGKS (2022). Legal Protection for Leakage of Consumer Personal Data in Marketplace Electronic Commerce. *Journal of Legal Preferences*, 3(1), 143

¹⁷ See Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE)

¹⁸ Olifiansyah, M. (2021). Legal Protection for Personal Data Theft and the Dangers of Using Online Loan Applications. *JOURNAL OF LAW DE'RECHTSSTAAT*, 7(2), 199

¹⁹ Ibid

marketplace can use Article 15 Paragraphs (1) and (2) as a legal basis for their lawsuit, which reads as follows:²⁰

1. Every Electronic System Operator must operate the Electronic System reliably and safely and be responsible for the proper operation of the Electronic System.
2. Electronic System Operators are responsible for the Operation of their Electronic Systems.

However, the provisions as stated in Article 15 Paragraph (1) are limited by the provisions in Article 15 Paragraph (3) which explains that Article 15 Paragraph (1) becomes invalid in the event that PSE can prove the existence of a force majeure, and/or an error / negligence on the part of electronic system users. Therefore, consumers who feel aggrieved as a result of the leakage of their personal data can use Article 15 Paragraphs (1) and (2) as a legal basis for their claims as long as the marketplace cannot prove the existence of a force majeure and fault/negligence on the part of the user/consumer.²¹

Even so, Law Number 11 of 2008 concerning Information and Electronic Transactions does not specifically explain the sanctions or penalties that can be imposed on PSE who violate the provisions of Article 15 Paragraphs (1) and (2). When viewed from Government Regulation Number 71 of 2019 concerning Implementation of Electronic Systems and Transactions which is a revision of Government Regulation Number 82 of 2012, in Article 3 Paragraph (1) of this PP PTSE requires PSE in the implementation of electronic systems to be carried out reliably, safely and responsible. Not much different from the provisions in Law Number 11 of 2008 concerning Information and Electronic Transactions namely that the provisions of Article 3 Paragraph (1) PP PSTE become invalid in the event of a force majeure event, and/or negligence of the user of the electronic system whose occurrence or negligence can be proven. As long as the two conditions for cancellation of Article 3 Paragraph (1) of PP PSTE cannot be proven as PSE, then the party charged with responsibility is PSE.²²

In this regard, Article 28 Letter c of the Minister of Communication and Informatics PDPSE explains that PSE is required to inform the owner of personal data about failures in protecting personal data in written form, with the following notification provisions; (a) must be accompanied by reasons or causes for the failure to protect the confidentiality of personal data; (b) can be done electronically if the owner of the personal data has given his consent which was stated at the time the acquisition and collection of his personal data was carried out; (c) it must be ensured that it has been received by the owner of the personal data if such failure creates a potential loss for the person concerned; and (d) a written notification is sent to the owner of the personal data no later than 14 (fourteen) days after the failure is known.²³

Article 3 of the PDPSE Permenkominfo regulates personal data protection. According to article 3 of the PDPSE Regulation of the Minister of Communication and Information, protection of personal data is carried out in the process; (a) acquisition and collection; (b) processing and analysis; (c) storage; (d) appearance, announcement, delivery, dissemination, and/or access opening; And; (e) extermination. Article 26 letter b explains that consumers as owners of personal data can submit complaints about failures to protect the confidentiality of personal data carried out by PSE to the Minister of Communication and Information of the Republic of Indonesia, then Article 29 paragraph (1) also states that owners of personal data and electronic system operators can submit a complaint to the Minister regarding the failure to protect the confidentiality of personal data.²⁴

The Role of Law in Marketplace Accountability for Data Leakage Cases in Indonesia in the Digital Dignitas Concept

In the digital era, personal data leaks are increasingly vulnerable²⁵. E-commerce companies have an obligation to prevent leakage of personal data by protecting the security of personal data from unauthorized access,

²⁰ See Law Number 11 of 2008 Concerning Information and Electronic Transactions (ITE)

²¹ Herryani, MRTR, & Njoto, H. (2022). Legal Protection Against Marketace Online Consumer Personal Data Leakage. *Legal Transparency*, 5(1).

²² Ibid

²³ See Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems

²⁴ Ibid

²⁵ Mochammad Januar Rizky, Risk of Data Leakage to Cyber Attacks, IJK Asked to Strengthen Digital Governance, accessed from Risk of Data Leakage to Cyber Attacks, IJK Asked to Strengthen Digital Governance (Hukumonline.com).

disclosure, alteration, misuse, destruction, and loss of personal data.²⁶ However, the lack of digital data security literacy and the absence of definite laws in digital crime opened the way for hackers to carry out their bad habits²⁷. Therefore, a legal umbrella is needed to handle cases of personal data leakage²⁸.

In the context of online marketplace liability for cases of data leakage in Indonesia, e-commerce companies or marketplaces have an obligation to prevent personal data leakage by protecting the security of personal data from unauthorized access, disclosure, modification, misuse, destruction, and loss of personal data. If there is a leak of personal data, the e-commerce company in question is required to provide written notification no later than three times twenty-four hours to its users and the institution that organizes personal data.²⁹ In the concept of digital dignity, leakage of personal data can harm users and violate their privacy rights³⁰. Therefore, marketplace companies must be responsible for leakage of user personal data and protect this personal data properly.

As we know, the concept of digital identity refers to the right to privacy and human dignity in the digital era³¹. The concept of digital dignity is closely related to the security of personal data because in the digital era, leakage of personal data can be detrimental to users and violate their privacy rights³². Therefore, marketplace companies must be responsible for leakage of users' personal data and protect these personal data properly. In addition, awareness of cybersecurity can have an impact on the security of personal data. Digital identity can also help protect personal data because users can control who can access their personal data. In maintaining the security of personal data, digital technology users must remain vigilant and careful in providing their personal information. Some tips and tricks that can be done to keep personal data secure in the digital era include ensuring data is encrypted, using strong passwords, and updating software regularly.³³

The role of law in marketplace accountability for cases of data leakage of marketplace users in Indonesia in the concept of digital dignity is to provide clear and transparent regulations, both in terms of the substance of the legal product and its implementation. There is a need for specific regulations governing this matter. So far, Indonesia does not have specific regulations related to the protection of personal data, although it is still separated into several different regulations which in fact still protect the realm of privacy in general. For example, article 26 of the ITE Law explains that personal data is part of a person's rights, which then explains the data in question can be seen in article 1 of PP PSTE. Then it is regulated in the next article in the ITE Law, namely articles 30-33 and article thirty-five. But alas, even though it has been regulated in such a way that the existing laws and regulations have not been able to accommodate the concerns of the public whose data has been taken illegally, especially the progress of AI technology in the marketplace which is growing rapidly and demands special regulations to be made so that the digital community is guaranteed their rights as citizens Indonesian country. As for the draft Law on Personal Data Protection, it has not shown its new moon to be ratified until now.

CONCLUSION

The conclusions that can be drawn from the description above are as follows The security of personal data of consumers using marketplaces in Indonesia is still not good, in fact there are still several principles that have not been fulfilled, such as the principle of limiting collection and security protection. Legal protection for the personal data of consumers who use marketplaces in Indonesia is reflected in existing laws and regulations, for example the ITE Law and PP PSTE. The role of law in marketplace accountability for data leakage cases in Indonesia in the concept of digital dignity is to provide special regulations that guarantee the fulfillment of people's rights. The concept of digital dignity is closely related to the security of personal data because in the digital era, leakage of personal data can be detrimental to users and violate their privacy rights. Therefore, marketplace companies must be responsible for leakage

²⁶ Nafiatul Munawarah SH., MH, E-Commerce Responsibility for Personal Data Leakage, accessed from E-Commerce Responsibility for Leakage of Personal Data (Hukumonline.com).

²⁷ ITS Online, accessed from Responding to Cases of Leakage of Personal Data in the Digital Age - ITS News.

²⁸ Edmon Makarim, Legal Responsibility for Leakage of Personal Data By: Edmon Makarim, Legal Responsibility for Leakage of Personal Data By: Edmon Makarim*) - Faculty of Law, University of Indonesia (ui.ac.id)

²⁹ Op. cit. Nafiatul Munawarah, SH., MH

³⁰ Ramiz Afif Naufal, Thesis, Responsibilities of PT. Tokopedia in Cases of Leakage of User Personal Data, 2020.

³¹ Op. cit. ITS Online

³² Aldi, The Importance of Maintaining Personal Data Security in the Digital Age, 2022 The Importance of Maintaining Personal Data Security in the Digital Age - UPT Information & Communication Technology (unri.ac.id)

³³ Batam Institute of Technology, Personal Data Protection in the Digital Age - ITEBA

of user personal data and protect this personal data properly. There are several suggestions that the author can give to solve the above problems, namely: In transactional activities on the marketplace, it is necessary to have supervision from a special party or a special institution to ensure the implementation of individual rights and the application of principles that are in accordance with current technological advances, because the marketplace security system is still minimal. There is a need for special regulations governing personal data protection, passing the PDP (Personal Data Protection) Bill is a good offer to guarantee legal protection for consumers who use marketplaces in Indonesia. In an effort to accelerate the digital dignitas concept in cases of personal data leakage in Indonesia it can be applied internally and externally, the intention is to educate the public as users of digital technology or marketplaces to remain vigilant and careful in providing their personal information and to the marketplace and the government can strengthen legal efforts and increase standards or standard clauses so that each marketplace has a balanced standard of security, in line with regulations and implementation.

ACKNOWLEDGMENT

The author would like to thank Annisa Hafizhah, S.H., M.H as a supervisor who has helped the author in completing the writing of this journal. Many challenges and obstacles were faced, but with Miss Annisa Hafizhah we can be completed this study and this journal can be read to this day. Hopefully the author can collaborate in the future with Annisa Hafizhah and other writers from various universities.

REFERENCES

- Aldi, The Importance of Maintaining Personal Data Security in the Digital Age, 2022 The Importance of Maintaining Personal Data Security in the Digital Age - UPT Information & Communication Technology (unri.ac.id)
- Amiruddin., and Zainal Asikin, Introduction to Legal Research Methods, Raja Grafindo Persada, Jakarta, 2014, p.47.
- Andre MR Wajong and Carolina Rizky Putri. 2010. "Security in Electronic Commerce." ComTech Vol 1 No 2 20.
- Angriani, P. 2021. Perlindungan Hukum terhadap Data Pribadi dalam Transaksi E-Commerce: Perspektif Hukum Islam dan Hukum Positif, DIKTUM: Jurnal Syariah dan Hukum Volume 19 Nomor 2 Desember 2021
- Batam Institute of Technology, Personal Data Protection in the Digital Age - ITEBA
- Central Bureau of Statistics, Central Bureau of Statistics (bps.go.id)
- CNN Indonesia, "E-Commerce Transactions Reach IDR 180.74 T as of September 2020" can be accessed on <https://www.cnnindonesia.com/economy/20201215150353-78-582406/transaksi-e-commerce-reach-rp18074-t-per-september-2020> accessed on May 21, 2023
- Edmon Makarim, Legal Responsibility for Leakage of Personal Data By: Edmon Makarim, Legal Responsibility for Leakage of Personal Data By: Edmon Makarim*) - Faculty of Law, University of Indonesia (ui.ac.id)
- Firman Hidranto, Encouraging G20 Sustainable Digital Transformation, accessed on Saturday, May 27 2023 at 21.00 WIB. -g20?lang=1
- Fitriani, Y., & Pakpahan, R. 2020. Analysis of Social Media Abuse for Spread of Cybercrime in Cyberspace or Cyberspace. Horizon, 20. <http://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala>
- Galuh Putri Riyanto, Third Largest Number of Marketplace Application Users in the World, accessed on Saturday, 27 May 2023 at 20.37 WIB., via Indonesia's Third Largest Number of Marketplace Application Users in the World Page all - Kompas.com.
- Herdi Setiawan, et al. 2020. "Legal Protection of Consumer Personal Data in E-Commerce Transactions" Merdeka Law Journal 104.
- Herryani, MRTR, & Njoto, H. 2022. Legal Protection Against Marketace Online Consumer Personal Data Leakage. Legal Transparency, 5(1).
- I Gusti Ngurah Indra Saputra, et al. 2017. "Development of Security Systems for E-Commerce." PIGEON VOL 5 NO 1 17.
- ITS Online, accessed from Responding to Cases of Leakage of Personal Data in the Digital Age - ITS News. Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE)
- M. Syamsudin, Legal Research Operations, Rajawali Press, Jakarta, 2007, p. 56-57
- Maichel Delpiro, et al. 2021. "Juridical Analysis of Privacy Policy and Online Market Place Accountability in the Protection of Users' Personal Data in Cases of Data Leakage." Padjadjaran Law Review Vol 9 No 1 32.

- Medan Area University Admin, The Role of AI in the World Economy, accessed on Saturday, 27 May 2023 at 20.30 WIB via [The Role of AI in the World Economy - \(uma.ac.id\)](#).
- Mochammad Januar Rizky, Risk of Data Leakage to Cyber Attacks, IJK Asked to Strengthen Digital Governance, accessed from [Risk of Data Leakage to Cyber Attacks, IJK Asked to Strengthen Digital Governance \(Hukumonline.com\)](#).
- Nafiatul Munawarah SH., MH, E-Commerce Responsibility for Personal Data Leakage, accessed from [E-Commerce Responsibility for Leakage of Personal Data \(Hukumonline.com\)](#).
- Natha, KDR, Budiarta, NP, & Astiti, NGKS. 2022. Legal Protection for Leakage of Consumer Personal Data in Marketplace Electronic Commerce. *Journal of Legal Preferences*, 3(1), 143
- Nidaul Khasanah, F., Samsiana, S., Trias Handayanto, R., Setyowati Srie Gunarti, A., Raharja, I., Raya, J., Raya Perjuangan, J., Mulya, M., Utara, B., & West, J. 2020. Utilization of Social Media and Ecommerce As Marketing Media In Supporting Independent Business Opportunities At During the Covid 19 Pandemic. 1(1), 51–62. <http://ejurnal.ubharajaya.ac.id/index.php/JSTPM>
- Olifiansyah, M. (2021). Legal Protection for Personal Data Theft and the Dangers of Using Online Loan Applications. *JOURNAL OF LAW DE'RECHTSSTAAT*, 7(2), 199
- PDP Bill Articles 59 and 68
- Ramiz Afif Naufal, Thesis, Responsibilities of PT. Tokopedia in Cases of Leakage of User Personal Data, 2020.
- Refer to the Basic Principles of National Application OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data Part Two Basic Principles of National Application
- Regulation of the Minister of Communication and Informatics Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems
- Reni Susanti, Artificial Intelligence: Definition, How it Works, Development and Impact, accessed on Saturday, 27 May 2023 at 20.22 WIB., via [Artificial Intelligence \(AI\): Definition, Development, How It Works, and Its Impact \(kompas.com\)](#).
- Reni Susanti, Rows of Personal Data Leakage Cases in the Last Two Years, accessed on Sunday, May 28 2023 at 09.00 WIB., via [Rows of Personal Data Leakage Cases in the Last Two Years... \(kompas.com\)](#).
- Riyadi, Gliddheo Algifariyano, Ringkasan Kebijakan CIPS (Center Of Indonesia Policy Studies), Ringkasan Kebijakan No. 7, Kerahasiaan Data Dalam Peraturan Perundang-Undangan Perlindungan Data Pribadi Di Indonesia, Meret 2021.
- Saputro, Prasetyo Dana. 2020. "Utilization of the E-Commerce Business To Consumer (B2C) Marketplace for the Development of Micro, Small and Medium Enterprises (MSMEs)." *Journal Knowlade Industrial Engineering* 4.
- Sinaga, Erlina Maria Christin, dan Mery Christian Putri, 2020. Formulasi Legislasi Perlindungan Data Pribadi Dalam Revolusi Industri 4.0, *Jurnal Rechtsvinding, Media Pembinaan Hukum Nasional*, Volume 9 Nomor 2,.
- SIRCLO, "Number of Indonesian E-Commerce Users in 2020 Increases Rapidly" can be accessed at <https://www.sirclo.com/blog/nomor-user-e-commerce-indonesia-di-tahun-2020-meningkat-pesat/> accessed on 21 May 2023.
- Soerjono Soekanto., and Sri Mamudji, Normative Legal Research; A Brief Overview, PT. Raja Grafindo Persada, Jakarta, 2003, p.13.
- Sugma, I Putu Bayu Mahandra and I Dewa Dana. 2020. "Protection of Personal Data of Online Consumers When Making Transactions in Indonesia." *Journal of Kertha Desa* Vol. 8 No. 12 p.42.
- Suratman., and Philips Dillah, Legal Research Methods, Alfabeta, Bandung, 2013, p.47
- Wulansari, Eka Martiana. 2020. Konsep Perlindungan Data Pribadi Sebagai Aspek Fundamental Norma dalam Perlindungan Terhadap Hak Atas Privasi Seseorang Di Indonesia, *Jurnal Surya Kencana Dua: Dinamika Masalah Hukum dan Keadilan* Vol. 7 Nomor 2, Sekolah Tinggi Ilmu Hukum/STIH Gunung Jati.
- Yan Andrianriza, et al. 2019. "Strategy for Implementing Personal Data Protection Regulation in Indonesia." Jakarta: Public Information and Communication Application Development Center HR Research and Development