International Journal of Education, Information Technology and Others (IJEIT), January 2024, 7 (1), 179-186
DOI: https://doi.org/10.5281/zenodo.10525368
p-ISSN: 2654-2528 e-ISSN: 2623-2324
Accredited by Directorate General of Strengthening for Research and Development
Available online at https://jurnal.peneliti.net/index.php/IJEIT

Legal Protection For Platform User Who Are Harmed By Data Leaks in E-Commerce and Prevention Efforts By The Government

Muhammad Iqbal Al Ikhsan[1], Rahmi Zubaedah[2]

[1,2]University of Singaperbangsa Karawang

Received: 15 December 2023
Revised: 28 December 2023
Accepted: 8 January 2024

Abstract

Personal data is what is most needed to process or carry out transaction activities on digital platforms. In processing, storing and managing personal data, it is not uncommon for failures in the system to result in personal data being leaked due to the inability of the electronic organizer to process the data, the electronic organizer's system being inadequate and a lack of security in the system. This research aims to determine the factors that cause leaks of personal data of platform users in e-commerce, legal protection for digital platform users who are accused of personal data leaks, and government efforts to reduce leaks of users' personal data in e-commerce. This research uses a normative juridical approach, namely an approach based on the main legal materials by examining legal principles, legal systematics and legal comparisons. Based on the research results, it can be concluded that the factors causing the leak of personal data of platform users in e-commerce are due to the lack of implementation of regulations, supervision of system suitability, education regarding the importance of protecting personal data, and cyber space security that is not well controlled, and the existence of forms of cyberspace threats. Preventive legal protection efforts in article 16 of Law Number 27 of 2022 concerning Protection of personal data, Article 26 paragraph (1) of Law Number 19 of 2016 concerning Electronic Information and Transactions, Article 33 Paragraph (2) of Government Regulation Number 80 of 2016 2019 Concerning Trading Through Electronic Systems. Repressive legal protection for users can be resolved through litigation or non-litigation based on Article 60 of the Personal Data Protection Law. The government's efforts to reduce data leaks include regulation, supervision and control, providing education, and securing cyberspace

Keywords: Personal Data, Data Leak, E-Commerce, regulations, cyberspace

(*) Corresponding Author: **muhammadiqbalalikhsan@gmail.com**

How to Cite: Al Ikhsan, M., & Zubaedah, R. (2024). Legal Protection For Platform User Who Are Harmed By Data Leaks In E-Commerce And Prevention Efforts By The Government. *International Journal of Education, Information Technology, and Others*, *7*(1), 179-186. https://doi.org/10.5281/zenodo.10525368

INTRODUCTION

Information technology, which is developing rapidly without being able to be prevented, has become a phenomenon that cannot be avoided. This is because humans always try to make activities easier to obtain information. Article 1 Number 3 of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, hereinafter referred to as the ITE Law, means information technology is a technique for collecting, preparing, storing, processing, announcing, analyzing and disseminate information.

The aim of information technology in Indonesia is to smarten the nation's life as part of the global information society, develop trade and the national economy in order to improve people's welfare and national economic growth

effectively and efficiently by prioritizing public services through optimal use of information technology to achieve justice and legal certainty and providing the widest possible opportunity for everyone to develop their thinking and abilities in the field of information technology responsibly

In the field of economics, promotions and potentials to improve people's welfare quickly without limitations of place, region and reach all levels of society, both nationally and internationally. Apart from that, in the field of E-commerce, recently it has become a necessity in buying and selling transactions, starting from daily necessities, lifestyle and current trends, which are very easy to access from home using the internet. Using this access is necessary. personal data, starting from name, cellphone number, home address, even personal accounts which are truly private.

Business actors or electronic system operators can collect personal data from customers or potential customers offline or online, offline is outside the network as a substitute for the word offline, while online is within the network or usually called online. Where digital data can be bought and sold without the knowledge and permission of the data owner or misused for purposes other than giving or handing over digital personal data), it can also happen that connected personal data is hijacked, stolen (hacked) by third parties.

Article 1 Number 1 of Law Number 27 of 2022 concerning Personal Data Protection, hereinafter referred to as the PDP Law, "Personal Data is any data about a person whether identified and/or identifiable individually or in combination with other information, either directly or indirectly. through electronic and/or non-electronic systems." Where personal data is one of the human rights which is part of personal protection, it is necessary to have a legal basis to provide security for personal data based on applicable laws.

The State guarantees the protection of personal data itself based on Article 1 paragraph 2 of the PDP Law, "personal data protection is the overall effort to protect personal data in the process of processing personal data in order to guarantee the constitutional rights of personal data subjects".

When looking at hackers' reasons for stealing personal data, financial gain is the biggest motive for hackers to hack. The financial crisis during the pandemic made everyone look for money in various ways. The high selling price of illegal personal data can make hackers earn millions to billions of rupiah every month.

In the case of leakage of personal data in online buying and selling transactions or E-commerce, namely the case of 91 million Tokopedia user data due to an error by Tokopedia as the electronic system organizer in storing and protecting the confidentiality of personal data and account privacy rights of users of the online shopping site Tokopedia.com which have been bought and sold on the internet. Tokopedia has made a mistake because it does not have a proper electronic system and does not have a proper security system to prevent leaks or prevent any unlawful processing or use of personal data.

To maintain confidentiality and protect personal data and the privacy of citizens who carry out electronic transactions, the state obliges every party who obtains personal data. Including acting as a trustee in storing and controlling someone's personal data.

REASEARCH METHOD

This research uses a normative juridical approach, which is meant by a normative juridical approach according to Soerjono Soekanto, namely legal research carried out by examining library materials or secondary data as basic material for research by conducting searches of regulations and literature related to the problem at hand researched.

The research specifications used in this research are descriptive analysis, namely research examining rules and regulations as well as legal theories related to the legal issues being handled, namely by examining problems from a legal perspective contained in the Personal Data Protection Regulations and Electronic Transaction Systems from the literature provided. relevant to the subject matter.

The data source used in this research is secondary data. Secondary data is data obtained from official documents, books related to research objects, research results in the form of reports, journals and statutory regulations.

RESULTS AND DISCUSSION

Legal protection is all efforts to fulfill rights and provide assistance to provide a sense of security to witnesses and/or victims, legal protection for crime victims as part of community protection, can be realized in various forms, such as through the provision of restitution, compensation, medical services and legal aid.

Then Phillipus M. Hadjon's theory is that legal protection for the people is a preventive and repressive government action. Preventive legal protection aims to prevent disputes from occurring, which directs government actions to be careful in making decisions based on discretion, and repressive protection aims to resolve disputes, including handling them in judicial institutions.

The leak of consumer personal data shows the urgency of strengthening personal data protection in Indonesia. This is further exacerbated by the minimal implementation of laws related to data protection so that there is legal certainty regarding the protection of consumers' personal data in Indonesia. The regulation of personal data in Indonesia is still general in nature and spread across several regulations, from various regulations governing the protection of personal data, without realizing it, this results in overlapping mechanisms and authority in protecting personal data so that the most disadvantaged are the users of the personal data.

The form of legal protection itself is to reduce misuse of personal data from users of personal data, forms of misuse of data that is leaked/not properly protected, as follows:

1. Personal data that is leaked or not properly protected can be used to break into someone's financial account.
2. Misuse of someone's personal data to make online loans.
3. Used for political interests by irresponsible parties.
4. Leaked personal data is used to hack the social media account of the owner of the personal data, so it has the potential to be misused for fraud or other crimes.

A. Legal Protection

The regulation of personal data protection in Law Number 27 of 2022 concerning the protection of personal data, which has a dignified justice perspective, namely has material, content, which reflects the nature and character of the Indonesian nation. The regulation of personal data has the value of justice for parties involved in technology, personal data, in this case it is mandatory to contribute to the protection of consumers and providers. Consumers in personal data have a weak position if they become victims because consumers are required to fight against large companies, which means that this arrangement has the value of equilibrium, harmony between national and international regulations.

Article 1 paragraph (2) of the Personal Data Protection Law provides clarification regarding the protection of personal data. "Personal data protection is the overall effort to protect personal data in the process of personal data processing in order to guarantee the constitutional rights of personal data subjects."

Enforcement of personal data protection laws is carried out from upstream (beginning) to downstream (end). Starting from the preventive side, prevention of misuse of personal data starts from the licensing side, system suitability, data processing, so the competent authority has the duty to play a significant role in registration and carry out national standardization selection for the administration of personal data.

Form of legal protection to prevent personal data leakage or preventive legal protection. Efforts to prevent data leaks are explained as in Article 16 of the PDP Law explaining the processing of users' personal data, namely the collection of personal data in a limited and specific manner, legally and transparently to guarantee the rights of personal data subjects. Processing is carried out accurately, up to date and responsibly. In processing personal data, the aim is to protect the security of personal data from unauthorized access, misuse, destruction and deletion of personal data. When processing personal data where protection fails, the personal data subject must be notified.

Articles 5 to 15 of the PDP Law discuss the rights of personal data users or personal data subjects, including the right to obtain clear information, the right to end personal data processing, the right to cancel consent, the right to sue and receive compensation.

Legal protection is repressive in nature, meaning it aims to resolve disputes, including handling them in court institutions, as explained in the personal data protection law. Article 67 of the PDP Law is:

a. Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person which may result in loss to the Personal Data Subject is subject to imprisonment for a maximum of 5 (five) years and/or a fine of a maximum of IDR 5,000. 000,000 (five billion rupiah).
b. Any person who intentionally and unlawfully discloses Personal Data that does not belong to him/her shall be subject to a maximum sentence of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000 (four billion rupiah).

c. Any person who intentionally and unlawfully uses Personal Data that does not belong to him or her will be punished by imprisonment for a maximum of 5 (five) years and/or a fine of a maximum of IDR 5,000,000,000 (five billion rupiah)."

Article 57 of the PDP Law explains administrative sanctions for leaks of personal data or failures in electronic administration systems, in the form of:

a. Written warning.
b. Temporary suspension of personal data processing activities.
c. Removal or destruction of personal data.
d. Administrative fines.

Article 60 of the PDP Law explains the government institutions that have authority over the management of personal data to realize the protection of personal data as well as enforce administrative law for violations and facilitate the resolution of disputes outside of court or non-litigation. This institution is appointed by the president.

Article 64 of the PDP Law explains dispute resolution and procedural law related to data leaks or data processing failures. Personal data protection dispute resolution is carried out through arbitration, court, or other alternative dispute resolution institutions. The procedural law that applies in dispute resolution or judicial processes is implemented based on statutory provisions. Valid evidence as regulated in the procedural law is in the form of electronic information and electronic documents. The trial process was carried out behind closed doors to protect personal data.

Criminal provisions for leakage of personal data are regulated in Article 70 of the PDP Law regarding the imposition of criminal penalties against corporations, as corporate criminal penalties are only fines and are imposed at a maximum of 10 (ten) times the maximum penalty stated. There are additional criminal penalties imposed on corporations, namely:

a. Confiscation of profits and/or assets obtained or proceeds from criminal acts.
b. Suspension of all or part of corporate business.
c. Closure of all or part of the business premises of corporate activities.
d. Carrying out obligations that have been fulfilled.
e. Payment of compensation.
f. Revocation of permission.
g. Dissolution of the corporation.

B. Dispute Resolution

In the case of leakage of personal data on the sales platform via the Tokopedia electronic system, PT Tokopedia has committed unlawful acts as a result of which personal user data has been spread due to being bought and sold by hackers. PT Tokopedia in the data leak case has taken legal action in a trial registered at the Central Jakarta District Court with Decision Number: 235/PDT.G/2020/PN.JKT.PST.

According to Article 64 of the PDP Law, legal settlement is carried out through arbitration, court, or other alternative dispute resolution institutions in accordance with statutory regulations. Procedural law applicable in dispute resolution and/or judicial processes for personal data protection is implemented based on applicable procedural law in accordance with statutory regulations. Evidence in the judicial process includes evidence in accordance with procedural law, other evidence in the form of electronic information and/or electronic documents in accordance with statutory regulations. In cases where it is necessary to protect personal data, the trading process is carried out behind closed doors.

Criminal provisions in the case of leakage of personal data are regulated in article 67 of the PDP Law, namely:

1. every person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or another person which may result in loss to the Personal Data Subject shall be sentenced to imprisonment for a maximum of 5 (five) years and/or a fine of a maximum of Rp. ,5,000,000,000 (five billion rupiah).
2. every person who intentionally and unlawfully discloses Personal Data that does not belong to them shall be subject to a maximum sentence of 4 (four) years and/or a maximum fine of Rp. 4,000,000,000 (four billion rupiah).
3. Any person who intentionally and unlawfully uses Personal Data that does not belong to him or her will be punished by imprisonment for a maximum of 5 (five) years and/or a fine of a maximum of IDR 5,000,000,000 (five billion rupiah).

In the case of the Tokopedia data leak, the criminal offense was imposed on the management, control holder, order giver, beneficial owner, and/or the corporation. The only punishment that can be imposed on a corporation is a fine. The fine imposed on the Corporation is a maximum of 10 (ten) times the maximum fine threatened. In the event of a data leak at Tokopedia, which is a large corporation and has a position in Indonesia, according to Article 70 of the PDP Law, there are additional penalties in the form of:

1. Confiscation of profits and/or assets obtained or proceeds from criminal acts;
2. Suspension of all or part of the Corporation's business;
3. Permanent prohibition on carrying out certain acts;
4. Closure of all or part of the Company's business premises and/or activities;
5. Carry out obligations that have been fulfilled;
6. Payment of compensation;
7. Revocation of permits and/or; and
8. Dissolution of the Corporation.

C. Government Efforts In Securing Cyberspace

In cyber security, on April 13 2021 there was regulation Number 28 of 2021 concerning the National Cyber and Crypto Agency or hereinafter referred to as the BSSN Presidential Decree. This publication is based on the need to restructure the

BSSN organization in order to realize National Cyber Security, Protection and Sovereignty and increase national economic growth.

In cyberspace, issues related to making profits in cyberspace often occur by irresponsible parties. Valuable information, one of which is personal data that should be safe and protected, has actually become an illegal commodity that is traded. In this case, BSSN is also part of maintaining the country's cyber security.

In carrying out security in cyber space, BSSN has its own function, according to Article 3 of Presidential Regulation Number 28 of 2021 concerning the National Cyber and Crypto Agency, explaining:

1. Formulating and establishing technical policies in the field of cyber and password security.
2. Implementation of technical policies in the field of cyber and password security.
3. Preparation of norms, standards, procedures and criteria in the field of coding.
4. Implementation of technical guidance and supervision in the coding field.
5. Coordination of task implementation, coaching and administrative support.
6. Management of State property is the responsibility of BSSN.
7. Implementation of substantive support to all organizational elements within the BSSN environment; and
8. Supervision of the implementation of tasks within the BSSN environment.

Indonesia's cyber security strategic objectives are achieving cyber resilience, public service security, cyber law enforcement, cyber security culture and cyber security in the digital economy. In order to achieve security and comfort in the digital space, the Cyber Agency was created to answer problems in the digital world.

The government continues to strive to reduce data leaks from the factors that cause data leaks. This strategic step aims to solve problems and provide protection for users of personal data.

CONCLUSION

Factors that cause leaks of personal data of digital platform users in e-commerce are the lack of implementation of legal regulations regarding personal data protection, the lack of supervision and internal control of companies and governments regarding the suitability of electronic system operators, the lack of related education and outreach. the importance of protecting personal data, securing cyber space that is not well controlled, as well as the existence of cyber space threats.

Legal protection for digital platform users who suffer losses due to leaks of personal data is protected in a preventive and repressive manner. Preventive legal protection, namely in Article 5, Article 12, Article 16 of Law Number 27 of 2022 concerning Personal Data Protection, Article 26 paragraph (1) of Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Article 33 Paragraph (2) Government Regulation Number 80 of 2019 concerning Trading via Electronic Systems. Repressive legal protection for users can be resolved through litigation or non-

litigation based on Article 60 of the Personal Data Protection Law. In accordance with the case above, repressive legal protection is through litigation settlement due to unlawful acts committed by electronic system operators which cause losses to users.

BIBLIOGRAPHY

Masitoh Indriani. (2005). Praktek Surveillance dan Unlawful Interception sebagai Pelanggaran terhadap Hak atas Privasi dalam Kebebasan Berekspresi di Indonesia: Hukum, Dinamika, Masalah dan Tantangannya. Jakarta: Eslam.

Sahar Maruli Tua Situmeang. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. Junal Sasi. Volume 27 No.1.

Nilam Andaria Kusuma Sari. (2017). Perlinfungan Privasi dan Data Pribadi Konsumen Daring pada Online Marketplace system. Justicia Jurnal Hukum. Volume 1 No.2.

Abdul Hakim Barkatullah. Perlindungan Hukum Bagi Konsumen Dalam Transaksi E-commerce Lintas Negara Di Indonesia. FH UII Press. Yogyakarta. 2009.

Angga Eka Yudha Wibawa. (2021) Implementasi Platform Digital Sebagai Media Pembelajaran Daring Di MI Muhammadiyah PK Kartasura Pada Masa Pandemi COVID-19. Berajah Journal Volume 1 No 2.

Edmon Makarim. Tanggung Jawab Penyelenggara Sistem Elektronik. Rajawali Press. Jakarta. 2010.

Ramiz Afif Naufal. Skripsi:Tanggung Jwab PT.Tokopedia dalam Kasus Kebocoran Data pribadi Pengguna. Universitas Islam Indonesia. Yogyakarta. 2020.

Muhammad Fathur. (2020) Tanggung Jawab Tokopedia Terhadap Kebocoran Data Pribadi Konsumen. Journal UPN Jakarta. Volume 2 No.2.

M.Alfari Yudha. (2023). Tanggung Jawab Penyedia Atas Keamanan Data Penggunaan Layanan Dalam Transaksi Online Melalui Tokopedia. Journal Notarius. Volume 2 No.1.

Phillipus M.Hadjon, Perlindungan Hukum Bagi Rakyat Indonesia. Bina Ilmu. Surabaya. 1987.

Sista Dewi. CyberLaw Perlindungan Privasi Atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional. Widya Pajajaran. Bandung. 2009.

Rizky P.P Karo-karo. Pengaturan Perlindungan Data Pribadi Di Indonesia Perspektif Teori Keadilan Bermartabat. Nusa Media. Bandung. 2020.