Journal Evidence Of Law
Vol 3 No 2 Mei-Agustus 2024
[1]Ivan Taffarel Almeyda, [2]Endang Prasetyawati
https://jurnal.erapublikasi.id/index.php/JEL

Consumer Protection for The Hacking of Personal Data of Tokopedia Marketplace Users

[1]Ivan Taffarel Almeyda, [2]Endang Prasetyawati
[1,2]University of August 17 1945 Surabaya
[1]ivantaffarel01@gmail.com, [2]endang_pras@untag-sby.ac.id

ABSTRACT

The issue of consumer personal data security that is vulnerable to hacking and misuse by irresponsible parties should be the main focus of the government through the establishment of Law Number 27 of 2022 concerning Personal Data Protection. The subject matter of this research is a case that occurred in Tokopedia e-commerce. Concerns about personal data security and privacy arose as a result of a data leak that occurred in May 2020, in which the data of 91 million Tokopedia user accounts were hacked and offered for sale on the Dark Web. From a sociological point of view, this event has the potential to reduce public trust in e-commerce platforms and digital technology as a whole. When data is leaked, consumers may become more wary and potentially reduce interest in online shopping for fear that their personal data will be stolen or misused. The subject matter of this research is how legal protection efforts can be provided against consumer personal data leaks in the Tokopedia Marketplace with a normative legal research method, also known as normative juridical research, will be employed in this study. The normative juridical research approach involves doing legal study solely through the examination of secondary data or library materials. Normative juridical research, sometimes known as the normative legal research method, is the approach method used in this writing. Library legal research using secondary data or library materials is known as normative juridical research.

Keywords: Consumer Protection, Personal Data Security and Privacy, Tokopedia Marketplace

ABSTRAK

Isu keamanan data pribadi konsumen yang rentan terhadap peretasan dan adanya pihak yang tidak bertanggung jawab melakukan penyalahgunaan harus menjadi fokus utama pemerintah melalui dibentuknya Undang-undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Isu utama dalam penulisan ini adalah kasus yang terjadi pada e-commerce Tokopedia. Kekhawatiran tentang keamanan dan privasi data pribadi muncul sebagai akibat dari kebocoran data yang terjadi pada Mei 2020, di mana data 91 juta user pemakai Tokopedia mengalami peretasan dan diperjualbelikan melalui situs gelap. Dari sudut pandang sosiologis, peristiwa ini berpotensi mengurangi kepercayaan masyarakat terhadap platform e-commerce dan teknologi digital secara keseluruhan. Ketika data bocor, konsumen mungkin menjadi lebih waspada dan berpotensi mengurangi minat terhadap belanja online karena khawatir data pribadi mereka akan dicuri atau disalahgunakan. Penelitian ini menjelaskan tentang bagaimana perlindungan hukum dapat diberikan bagi pengguna akun yang mengalami kebocoran data pribadi konsumen Tokopedia dengan metode penulisan yang digunakan adalah pendekatan penelitian normatif. Penelitian yuridis normatif—juga dikenal sebagai metode normatif—merupakan metode penelitian hukum yang melibatkan acuan bahan hukum sekunder atau bahan kepustakaan. Dalam penulisan artikel ini, metode ini digunakan.

Kata Kunci: Data Pribadi, Marketplace Tokopedia, Perlindungan Konsumen

Introduction

Information and communication technology has affected various aspects of people's lives, including government, business, education, health, and personal life. While this technology provides positive benefits, it also allows opportunities for cyber crime. Unlawful acts in cyberspace, such as carding, fraud, data hacking, terrorism, and dissemination of destructive information, have become a very worrying phenomenon. Therefore, information and communication technology can be considered as a double-edged sword that contributes positively to human progress, but also becomes an effective means to commit unlawful acts. The issue of consumer personal data security that is vulnerable to hacking and misuse by irresponsible parties should be the main focus of the government. This is a serious problem that can result in criminal acts such as fraud and defamation, where the perpetrator uses the victim's identity without authorization. As a result, individuals whose personal information is hacked may be wrongly accused of crimes they did not commit.

Information about a customer's identify is known as personal data, characteristics, and behavior of consumers collected, processed, and stored by *e-commerce* providers. Names, addresses, phone numbers, email addresses, credit card numbers, transaction histories, preferences, and other information are examples of personal data. Consumer personal data has high economic value and can be used for various purposes, both legitimate and illegitimate (Indriani Muin, 2023). Consumer personal data leakage is an event where consumer personal data is disseminated, accessed, altered, or misused by unauthorized parties without consumer consent. Consumer personal data leakage can occur due to various factors, such as cyber attacks, negligence, errors, or crimes by *e-commerce* providers or third parties involved in *e-commerce* transactions. Leakage of personal data can negatively impact on consumers, such as financial loss, identity theft, fraud, harassment, discrimination, or privacy intrusion (Deanne Destriani Firmansyah Putri, 2020). Consumer protection against *e-commerce* personal data leakage is an effort to keep customer personal data accessible, secure, and confidential and provide rights and responsibilities for consumers and *e-commerce* organizers in managing consumer personal data. Consumer protection against *e-commerce* personal data leakage includes legal, technical, and social aspects. Legal aspects relate to regulations and law enforcement mechanisms governing the collection, processing, storage, use and protection of consumer personal data. The technical aspect relates to the use of secure and standardized information and communication technology in the management of consumer personal data. The social aspect relates to awareness, participation, and education for consumers and *e-commerce* providers about the importance of consumer personal data protection (Achmad Thorik, 2023).

The issue of consumer protection against *e-commerce* personal data leakage is becoming increasingly relevant and urgent in Indonesia, given the rapid development of *e-commerce* and the lack of certain rules pertaining to the protection of personal data. Therefore, this research aims to review and analyze consumer protection against *e-commerce* personal data leakage in Indonesia, with a case study of Tokopedia *e-commerce.* We anticipate that this research will help the development of policies and practices of consumer personal information security in Indonesia, especially in the context of *e-commerce*. Law as a scientific discipline has a very important role in regulating social life. In its development, law continues to undergo changes and adjustments to be able to answer the challenges of the times. Therefore, legal research is a necessity to explore and understand the dynamics and development of law. In the context of Indonesian law, some of the important regulations relating to marketplaces include 'Law Number 11 of 2008' on Electronic Information and Transactions (UU ITE) as amended by Law

Number 19 of 2016, as well as regulations issued by the Ministry of Trade and other relevant agencies. Personal data leaks can lead to various legal issues, including breaches of the private rights of consumers and potential misuse of data. In the event of a leak, Customers are entitled to legal protection and may pursue legal action through both litigation and non-litigation channels. Corporate actors are also accountable for paying damages in the event that a negligence-related breach of customer personal data occurs, as well as for protecting the confidentiality and integrity of that data.

The issue of safeguarding individual privacy and ensuring the integrity of personal information. arose as a result of a data leak that occurred in May 2020, in which the data of 91 million Tokopedia user accounts were hacked and sold on *Dark Web* sites. From a sociological point of view, this event has the potential to reduce public trust in *e-commerce platforms* and digital technology as a whole. When data is leaked, consumers may become more wary and potentially less interested in online shopping for fear that their personal data will be stolen or misused. Data leaks can also spark debates in society about the importance of personal data protection and stricter government regulations to protect consumer rights. The data leak could also show how important it is for people to become digitally aware to know and protect themselves from the risks of cybersecurity threats. Overall, Tokopedia's data leak is not just a technical issue; it also has social consequences, affecting social interactions and consumer trust in the digital economy.

Methods Research

In this research, the title and problems to be discussed will be answered using normative juridical research methods. This method is in the form of library legal research that only uses secondary data and library materials. In this proposal, the approach used is the normative juridical research method, which is also in the form of library legal research that only uses secondary data and library materials (Efendi, J., 2016). By using the deductive thinking method, which involves drawing conclusions from general and correct conclusions, the object of analysis using a qualitative approach is research based on legal norms contained in laws and regulations.

Results and Discussion

Legal Protection Efforts That Can Be Provided Protecting Consumer Personal Information from Disclosure in the Tokopedia Marketplace

In the case of the Tokopedia data leak, the company initially avoided and did not admit to the leak. However, after an investigation by cybersecurity and evidence found on Twitter, Tokopedia finally admitted that user data was leaked. The chronology of events began when a hacker by the name of Whysodank published the results of the hack on the Raid Forum on March 20, 2020. Then, the @underthebreach account announced the hack on Twitter and claimed to be an Israeli security surveillance service. The tweet immediately received a response from Indonesian users. Tokopedia later acknowledged an attempt to steal user data, as stated by Nuraini Razak, VP of Corporate Communications Tokopedia. The next day, Whysodank announced the sale of 91 million user data on a darkweb forum called EmpireMarket under the account name ShinyHunters. This data invalidates previous claims of only 15 million accounts. The Hackread site then uploaded the hack of 91 million Tokopedia accounts and revealed that the leaked accounts were sold for IDR 74 million. The Tokopedia data leak incident began with a hack by Whysodank at Raid Forum on March 20, 2020. Then, the @underthebreach account announced the hack on Twitter and claimed to be an Israeli

security surveillance service. Tokopedia was initially evasive, but after an investigation, the company acknowledged the data leak. The next day, Whysodank announced the sale of 91 million user data on a darkweb forum under the account name ShinyHunters, disputing previous claims of only 15 million accounts. The Hackread website later uploaded the hack of 91 million Tokopedia accounts and revealed that the leaked accounts were sold for IDR 74 million.

Legal protection of consumers is a must that is guaranteed by business actors, as specified by the consumer protection law. The right to protection has been stated in the 1945 Constitution of the Republic of Indonesia, Article 28 G paragraph 1, which states believe everyone is entitled to the defense of their person, family, honor, dignity, and property. They also have the right to a feeling of security and defense against intimidation into doing or refraining from acting in accordance with their human rights.Consumer protection can be in the form of economic, social, and political protection. However, legal protection is the most important and the focus of this discussion. Legal protection is the main form of protection because the law can accommodate the interests and rights of consumers comprehensively. In addition, the law has a coercive power that is officially recognized in the state, so it can be implemented permanently. In practice, legal protection of consumers can be in the form of protection from crime, fraud, and the use of unsafe products. Consumers are also entitled to compensation in the event of losses due to products that do not meet specifications. Legal protection can also be as an example of protection from Unauthorized access to personal information, as well as protection from discriminatory actions in business transactions, legal protection of consumers is a must that is guaranteed by business actors and regulated in consumer protection laws.

Legal protection is the main form of protection because the law can accommodate the interests and rights of consumers comprehensively and has the power of force that is officially recognized in the state. Legal protection may take the shape of protection from crime, fraud, and the use of unsafe products, as well as protection from unauthorized and discriminatory use of personal data in business transactions. The word protection linguistically has similarities or similar elements, namely:

1) The protective action aspect;
2) The protecting parties element; and
3) The measures to protect element.

Thus, the term protection has a broader meaning, namely an action or effort to protect certain individuals or groups from threats or dangers posed by other parties. The definition of protection shows that overall, protection can cover various aspects, including protection from criminal acts that endanger, interests, or inanimate objects. The term "protection" can also refer to all actions taken by the government to provide legal clarity and offer the community's citizens protection. In this context, protection can be in the form of policies set by the government to protect the rights of citizens and prevent violations of the law (Aldo sonjaya, 2022). Protection has a broader meaning, namely an action or effort to protect certain individuals or groups from threats or dangers. Protection can be in the form of policies set by the government to protect the rights of citizens and avoid breaking the law. The state also has clear rules in order to guarantee legal clarity and safeguard citizens, and avoid breaking the law by imposing sanctions according to existing regulations. So it is important that there is a law that protects personal data so that the leakage or when personal information is shared, it might lead to harm to the owner of the data. In addition, personal data is also included in the constitutional rights of Indonesian citizens so that the state has an obligation to provide legal protection, legal certainty, legal justice, and legal expediency for its people. The existence of

these regulations regarding the protection of victims of personal data leaks of Tokopedia users is expected to prevent personal data leaks / theft of personal data that occurs again in *all e-commerce* in Indonesia.

Tokopedia's Legal Responsibility for Consumer Personal Data Leakage

Article 26 of 'Perkominfo' No. 20/2016 regulates the rights of personal data owners. The rights in question are as follows:

1) The right to the privacy of one's personal information;
2) Complain to the Minister in the context of resolving disputes involving one's personal information about the Electronic System Operator's breach of that information's confidentiality;
3) Acquire the ability to access, amend, or update their data without interfering with the operation of the personal data management system, unless specifically permitted by applicable laws and regulations;
4) Get access to, or the chance to get, historical Personal Data that has been provided to the Electronic System Operator in compliance with legal and regulatory requirements; and
5) In the event that laws and regulations dictate differently, requesting the deletion of his or her Identified Individual Data from the Electronic System under the control of the Electronic System Operator.

This rule governs the duties owed to users of personal data as well as the rights of personal data owners. The duties at issue are:

1) Preserve the privacy of any personally identifiable information that is gathered, processed, and examined.
2) Utilize Personal Information solely as needed by the User;
3) Prevent abuse of personal data and the documents that contain it; and
4) accountable for any misuse of personal data within his or her power, whether through organizational control or individual control.

According to 'Law Number 27 Year 2022' on Personal Data Protection, one of the main objectives of this Law is the proper privacy protection the objectives of data owners. The rights of data owners that need to be considered include, among others:

1) The right to ask the person in charge of managing their personal data for appropriate access and copies of that data;
2) The right to request that the personal data manager update and rectify any mistakes or inconsistencies in the personal data that is under their administration;
3) The right to complete personal and data before the personal and data is managed by the personal data manager;
4) the ability to ask the management of personal data to delete the data;
5) the right to pursue compensation for rights abuses and to have those claims acknowledged;
6) The right to be able to withdraw at any time the data management consent that has been given to the data manager with notice.

In an agreement, the agreement between the parties will produce legal consequences through the relevant rights and obligations. In e-commerce, contracts which take place between buyers and sellers are not only in the form of contracts agreed orally or in writing, but also using digital data or digital messages that are not recorded on paper, known as paperless contracts. The existence of an e-commerce contract arises because of the equality of will between the seller and the buyer. An e-commerce contract occurs when the seller presents a form containing the contents of the contract and the buyer agrees to the contents of the

contract by using a check mark or clicking the "accept" button as a sign of approval. This creates equality of will between the seller and the buyer, so that the contract can be considered as a valid and applicable agreement. According to Alice, an agreement in an agreement will produce legal consequences in the form of rights and obligations between the parties. In e-commerce, the contract that occurs between the seller and the buyer is not only in the form of a contract agreed orally or in writing, but also using digital data or digital messages that are not recorded on paper. The existence of an e-commerce contract arises because of the equality of will between the seller and the buyer, which is indicated by the buyer's agreement to the contents of the contract using a check mark or clicking the "accept" button (Alice Kalagi, 2015). Terms and Conditions are rules set by Tokopedia as a service provider, which regulate the utilization of services associated with the www.tokopedia.com website. Users who register on the www.tokopedia.com/terms website and/or use it are considered to have read, understood, and agreed to the terms and conditions a click-wrap agreement, as the terms and conditions are also known, serves as the parties' electronic agreement (e-contract). When a customer clicks on the agreement part of an e-contract, an agreement is made. A contract for the purchase of products or the use of products or services provided by an online retailer is known as a "click-wrap agreement.". Before completing the transaction, online buyers are generally required to click on icons that say "I agree," "I accept," "OK," or "Agree" to indicate their agreement to the terms included in the established standard contract.

Tokopedia's Terms and Conditions are rules governing the utilization of services associated with visiting www.tokopedia.com. Users of the website are presumed to have read, understood, and consented to the terms and conditions. These terms and conditions serve as a click-wrap agreement, which is a type of electronic contract. When a consumer clicks the permission area of an e-contract, an agreement is made. Before completing the transaction, the online shopper must accept the terms stated in the standard contract (Muhammad Fathur, 2020). Based on the Consumer Protection Law, corporate actors have the following sorts of obligation:

1) Business actors are accountable for paying damages, clean-up costs, and/or losses suffered by consumers as a result of using manufactured or traded goods and/or services;
2) Advertising companies are in charge of creating the commercials and handling any fallout from them;
3) Should the items be imported without the assistance of an agent or representative of the foreign manufacturer, the importer bears responsibility as the importer's manufacturer;
4) Business actors who trade services are obliged to fulfill the agreed and/or promised guarantees and/or warranties;
5) Proof of the existence or absence of elements of guilt in criminal cases is the burden and responsibility of the business actor without closing the possibility for the prosecutor to carry out the proof.

A crucial topic in the study of consumer protection law is the concept of accountability. Analyzing who should bear blame and how much of it may be placed on the parties involved in consumer rights violations requires caution (Sidharta, 2004). The legal responsibility principles might be distinguished as follows (Inosentius Samsul, 2004):

a. The subjective concept of blame liability states that a business actor's actions decide who is liable. This principle is commonly used in criminal and civil law, and is firmly established in the Civil Code (KUHPerdata). This rule states that someone can only be held legally accountable if they have some degree of fault.;

b. The product liability concept is another name for the strict liability principle. Product liability refers to the manufacturer's obligation for goods sold to consumers that result in losses because of inherent flaws in the product.
c. According to the presumption of responsibility premise, the accused party is always presumed to be liable, until the defendant can prove his or her innocence. This principle applies to the reverse burden of proof (omerking van bewijslast). The principle of reversing the burden of proof is based on the presumption of innocence until and unless proven guilty. In consumer protection actions, the business being sued has the burden of demonstrating its innocence by providing proof of its innocence;
d. In contrast to the presumption of liability concept, there is an assumption of non-liability principle. This rule, which is typically common sense, is only acknowledged in a relatively narrow range of consumer interactions.
e. The limited liability principle is the opposite of the presumption of liability. In the context of law, responsibility is defined as strictly related to rights and obligations. Businesses strongly want that this principle be incorporated into standard agreements as an extenuation clause.

Tokopedia's liability for consumer personal data leaks is based on the ITE Law and the latest regulation, namely Law Number 27 of 2022 concerning Personal Data Protection. Tokopedia has made all efforts to protect electronic systems and implement risk management in accordance with applicable laws and regulations. If Tokopedia consumers feel harmed by this case, they can hold Tokopedia accountable through legal channels. Tokopedia as the largest e-commerce in Indonesia will comply with Indonesian law and is ready to take responsibility if something goes wrong. Administrative penalties including written warnings, fines, temporary suspensions, and access terminations can be used to enforce this responsibility. In addition, accountability can also be carried out civilly through a court lawsuit. Tokopedia has moved quickly to fix the existing loopholes of the security system and immediately provide information to all Tokopedia users. The appropriate efforts have been made to guarantee that accounts and transactions are kept, and the investigative process has commenced. Tokopedia has designated a top-tier independent organization with expertise in cybersecurity to support the investigation and identification of essential actions to further enhance the data protection of Tokopedia users. Tokopedia also makes sure that passwords are encrypted using one-way encryption.

Tokopedia's liability for consumer personal data leaks based on the ITE Law and the latest regulations. Tokopedia has made every effort to protect electronic systems and implement risk management in accordance with applicable laws and regulations. If Tokopedia consumers feel aggrieved, they can hold Tokopedia accountable through legal channels. Tokopedia has moved quickly to fix the existing loopholes of the security system and has appointed a world-class independent institution to help investigate and improve the data protection of Tokopedia users. To prevent data leakage cases like this from happening again, Tokopedia will strengthen the security system regularly. In addition, Penetration tests must be carried out regularly to find out where the security holes are. Marketplace sites like Tokopedia will always be targeted by hackers because they collect public data, especially credit cards, debit cards, and digital wallets. Investment funds received from investors will be used more for cyber security.

The use of encryption should be evenly distributed to all data related to users. This data leak case opens the eyes of all of us that data is very important to protect because personal data is a personal asset which if misused will have a very dangerous impact. Therefore, Tokopedia will always conduct socialization for all users to follow the recommended security

measures so that everything remains protected. The security measures that must be followed include ensuring regular password changes for Tokopedia accounts, not using the same password on various digital platforms, and maintaining OTP by not providing the OTP code to any party, including those on behalf of Tokopedia and for any reason.

Dispute Resolution Efforts Against Consumer Personal Data Leakage in the Tokopedia Marketplace

Proper dispute resolution is the desire of every party involved in the dispute, including consumers and business actors/producers. The dispute resolution mechanism can be chosen by the parties, either through the court or outside the court. However, dispute resolution between consumers and businesses/producers is sometimes deemed inappropriate due to the unbalanced position of consumers and businesses/producers as parties to the dispute. Consumers usually do not have the same resources as businesses/producers, so they tend to be victimized in the dispute resolution process.(Intan Nur Rahmawati & Rukiyah Lubis, 2014). Appropriate dispute resolution is the desire of every party involved in the dispute. The dispute resolution mechanism can be chosen by the parties, either through the court or outside the court. However, dispute resolution between consumers and business actors/producers is sometimes deemed inappropriate due to an imbalance in position. The existence of dispute resolution space in the consumer sector is a good policy in an effort to empower consumers. Efforts to strengthen or empower consumers are a form of awareness of the special characteristics of the consumer world, namely the existence of sharp differences in interests between two parties who have differences in their *bargaining* position.

However, based on the provisions in accordance with 'PERKOMINFO Number 20/2016', it is stated that 'Article 29 paragraph (2)' explains the purpose of making a complaint, namely to resolve disputes that occur in deliberation or through other dispute resolution efforts. 'Article 29 paragraph (3)' explains the reasons for making a complaint as referred to in paragraph (1). 'Article 29 paragraph (4)' explains the Minister's action in response to the complaint. The complaint as referred to in 'Article 29 paragraph (1)' is made based on the provisions of 'Article 31 letters a, b, c, and e'. followed by 'Article 30 paragraph (1)' which explains the further actions taken by the Minister when receiving complaints related to 'personal data disputes'. Based on 'Article 30 paragraph (1)' the Minister will delegate the authority to resolve personal data disputes to the Director General. Article 30 paragraph (2) explains that after the Director-General receives the delegation of power from the Minister regarding the settlement of personal data disputes, based on this paragraph, the Director-General has the authority to establish a personal data dispute resolution panel.

Article 31 letter a provides a time limit for complaints, complaints must be made no later than 30 working days after the complainant knows the information as referred to in Article 29 paragraph (3) letter a or b. Article 31 letter b requires complaints to be submitted in written form which contains information related to the name and address of the complainant, the reason for the complaint, the request for resolution of the problem complained of, and the place of the complaint, the time of submission of the complaint and the signature of the complainant. Article 31 letter c states that supporting evidence must be provided. Article 31 letter e states that incomplete complaints must be completed by the complainant with a time limit of 30 working days since the complainant receives a response that the complaint is incomplete. The settlement of personal data disputes with complete complaints as referred to in Article 31 letter f is carried out by deliberation or through other alternative dispute resolution efforts in accordance with the provisions of laws and regulations, this is regulated

in Article 31 letter g. Article 31 letter h explains that the personal data dispute resolution panel can provide recommendations to the Minister for the imposition of administrative sanctions on PSE, this recommendation is given regardless of whether the complaint can or cannot be resolved through deliberation or through other alternative dispute resolution efforts.

Article 32 Paragraph (1) explains that regarding efforts to resolve disputes by deliberation or through other alternative resolution efforts have not been able to resolve disputes over failures to protect the confidentiality of personal data, each data owner and electronic system organizer can file a lawsuit over the occurrence of failures to protect the confidentiality of personal data. In Article 32 Paragraph (2): The lawsuit as referred to in Paragraph (1) shall only be in the form of a civil lawsuit and shall be filed in accordance with laws and regulations.

There are several efforts to make this happen well, including:

1. Strengthening the Legal and Regulatory Framework
    a) Implementation of the Personal Data Protection Law (PDP Law): Ensure that the comprehensive PDP Law is properly implemented, providing a strong legal basis for consumers to assert their rights.
    b) Clear Implementing Regulations: Issue detailed implementing regulations for the PDP Law, outlining procedures for complaints, dispute handling, and sanctions for violators.
2. Internal Regulation and Enforcement at Tokopedia
    a) Transparent Privacy Policy: Ensure Tokopedia's privacy policy is clear and easy to understand, and informs consumers about their rights and how their data is protected.
    b) Data Security and Compliance Team: Establish a dedicated team responsible for data security and regulatory compliance, as well as handling data leakage incidents.
    c) Routine Security Audits: Conduct regular security audits to detect and mitigate potential vulnerabilities in the system.
3. Dispute Resolution Mechanism
    a) Consumer Complaint Service: Provide easily accessible complaint channels for consumers who experience data leakage, with prompt and effective responses.
    b) Mediation and Arbitration: Using mediation and arbitration mechanisms to resolve disputes amicably and efficiently, before proceeding to legal channels.
    c) Data Protection Committee: Establish an independent committee tasked with handling data protection-related disputes and recommending solutions.
4. Education and Awareness Raising
    a) Education Program: Conduct education programs for consumers on their rights regarding personal data and how to protect their personal information.
    b) Awareness Campaign: Conduct awareness campaigns on the importance of personal data protection and how to avoid the risk of data leakage.
5. Cooperation with Government and Non-Government Institutions
    a) Collaboration with the Ministry of Communication and Information: Work with the Ministry of Communications and Information Technology to ensure regulatory compliance and handling of data leakage incidents.
    b) Partnership with Consumer Protection Agencies: Collaborate with consumer protection organizations such as the Indonesian Consumer Rights Foundation (YLKI) to assist affected consumers and provide advocacy.

6. Use of Security Technology
    a) Implementation of Encryption Technology: Using encryption technology to protect consumers' personal data when transmitted and stored.
    b) Intrusion Detection System: Implement an intrusion detection system to detect and respond to security threats in real-time.
    c) Strict Security Protocols: Ensure all processes involving personal data follow strict security protocols, including multi-factor authentication and limited access management.
7. Transparency and Reporting
    a) Data Leak Incident Report: Requires Tokopedia to report data leakage incidents to authorities and affected consumers in a transparent and timely manner.
    b) Public Announcement: Publicly announce the steps taken to address the incident and prevent recurrence in the future.

Efforts to Improve Personal Data Protection for *Marketplace* Users

As internet usage increases, so do digital crimes. Therefore, a strong legal umbrella is needed to create better security. Vigilance against cybercrime must be put forward because the purpose of data theft is usually used to carry out fraud modes, data tapping, hacking, email spaming, and also manipulation of other people's data (phishing), which will then result in both material and immaterial losses to certain individuals and groups. Actualy, the figures who play an important role in maintaining privacy against personal data protection are the data owners themselves. When using social media or shopping online in the marketplace, data owners must understand the code of ethics and procedures for using it. We must also know about what we can and cannot do so that unwanted things do not happen in the future. This is useful as a form of prevention of crimes that will occur. Do not let regulations and other parties play their role, but the data owners do not comply with the rules or even expose their own personal data. When registering an account on an electronic trading platform, users are required to fill in personal information needed for administrative purposes before they can use the services of the platform.

This personal information includes full identity data and phone numbers, along with other required information. As part of the e-commerce platform's feature development and advancement, users are also required to upload a photo of their ID card and a selfie with their hand holding the ID card, as well as sign online. Thus, the e-commerce platform can ensure the security and privacy of user data, and prevent digital crimes that can cause material or immaterial losses. All of this information is part of the user's personal data that must be protected. The *marketplace plays* a role in personal data protection efforts in several ways:

a) preventive by providing multiple layers of user-enabled security such as OTP and encryption.
b) Adaptive is to conduct periodic checks on the platform's data security system, such as privacy impact assessment (PIA).
c) Collaborative Cooperate and consult with the government in an effort to realize personal data protection in accordance with applicable regulations in Indonesia.

In ensuring the security of consumers and electronic system providers, it is very necessary to pay attention to the granting of reliability certificates including 3 categories that determine the level of reliability certificates, namely as follows:

1. Identity registration is a certificate of reliability that guarantees the security that the identity of the business actor is true and trustworthy. This means that business actors

have verified and validated their identity, so that consumers can be sure that they are transacting with legitimate and trusted business actors.

2. Electronic system security, which is a certificate of reliability that guarantees reliability, provides certainty that the process of delivering or exchanging data through the business website is safe and secure. This means that the business's electronic system has been equipped with adequate security technology, so that consumer data can be protected from security threats such as hacking, phishing, and others.
3. A privacy policy is a certificate of reliability that provides assurance that consumers' personal data is properly protected. This means that the business has committed to protecting consumers' personal data in a manner that complies with applicable laws and security standards. For example, an "online buying and selling" business that has received a category 2 certificate of reliability by electronic system security can be trusted or believed to be safe when consumers exchange data in the service.

Here are some important aspects to consider to ensure the safeguarding of personal customer information:

1. Clear Privacy Policy: Every *e-commerce platform* should have a clear privacy policy that is easy for users to understand. This document should explain how personal data is collected, used, stored, and protected by the *platform*.
2. User approval: Before collecting or using users' personal data, it is crucial to have their approval. This contains details regarding cookies, email addresses, payment methods, and more personal information gathered from users while they interact with the online store.
3. Data Security: Strong security measures must be implemented by e-commerce platforms to safeguard consumers' personal data from unauthorized access, hacking, or misuse. This includes data encryption, use of proper security protocols, and regular security monitoring.
4. User Access to Their Data: Consumers should have easy access to view, update, or delete their personal data stored by the *e-commerce platform*. This allows them to have control over their personal information and ensure the accuracy of the data stored.
5. Transparent Use of Data: The use of Personal information must be open and compliant with the established privacy policy. *E-commerce platforms* should avoid using data for purposes that are not appropriate or not disclosed to users.
6. Regulatory Compliance: *E-commerce platforms* must comply with all applicable regulations and laws related to personal data protection, both at national and international levels.
7. User Education: Users need to be made aware of the significance of protecting their personal data and the steps they can take to protect their personal information when interacting with *e-commerce platforms*.

The Indonesian government itself has taken several steps in an effort to improve the safeguarding of private information of *marketplace* users. Here are some of the efforts that have been made:

1. Regulations and Policies: The government has issued various regulations and policies related to personal data protection, such as the Minister of Communication and Information Technology Regulation (Permenkominfo) No. 20/2016 on Personal Data Protection in Electronic Systems. This regulation provides a clear framework for the protection of personal data of marketplace users.

2. Establishment of Supervisory Body: The government has established the Personal Data Protection Supervisory Board (BPDP) as the agency responsible for overseeing the implementation of personal data protection regulations in Indonesia. The BPDP has an important role in enforcing compliance with these regulations.
3. Education and Awareness: The government has also made efforts to raise awareness about the importance of personal data protection among *marketplace* users. This is done through education and socialization campaigns organized by various government agencies, non-governmental organizations, and technology companies that can be:
    a) Awareness Campaign: Carry out widespread public awareness campaigns to improve people's understanding of the importance of personal data protection and how to protect their personal information.
    b) Training and *Workshop*: Conduct training and workshops for users and businesses in the marketplace on best practices in maintaining personal data security.
    c) Education Curriculum: Incorporate personal data protection and digital security topics into school and university education curricula.
4. Cooperation with Industry: The government is working with the marketplace industry to improve personal data protection practices. This includes holding dialogs and consultations with technology companies to discuss issues related to data security and privacy.
5. Monitoring and Law Enforcement: The government is active in monitoring and enforcing the law against personal data protection violations. The Personal Data Protection Supervisory Agency (BPDP) has the authority to investigate personal data violations and sanction violators. In addition, rights and mechanisms for consumer complaints should also be implemented:
    a) Right of Access and Data Correction: Gives consumers the right to access, correct, and delete their personal data stored by the *marketplace*.
    b) Effective Grievance Mechanism: Provide an easily accessible and responsive grievance mechanism for consumers who feel their personal data has been misused or breached. Marketplaces should have clear procedures for handling and resolving such complaints.
6. Cooperation and Collaboration:
    a) Collaboration between Government Agencies: Enhance cooperation between the Ministry of Communications and Informatics, the Financial Services Authority (OJK), and the National Cyber and Crypto Agency (BSSN) to oversee and regulate personal data protection in the digital sector.
    b) Partnership with Private Sector: Encourage partnerships between the government and the private sector to develop better data security standards and share best practices in personal data protection.
    c) International: The government also engages in international collaboration in an effort to improve personal data protection. This includes cooperation with other countries in exchanging information and experiences related to personal data protection regulations.

With these efforts, the Indonesian government hopes to create a safer and more reliable environment for marketplace users, as well as increase public trust in e-commerce services in Indonesia. By doing so, consumers will feel more comfortable and confident to transact online, thereby increasing consumer participation, sales volume, and national economic growth.

With the enactment of the Personal Data Protection Law, it centers on broad guidelines for protecting personal data, whether it is processed entirely or in part using both electronic and non-electronic methods. Based on the unique characteristics of each industry, personal data protection can be implemented in every area. The goals of the Personal Data Regulation are to, among other things, safeguard citizens' fundamental rights to privacy protection, ensure that the public can access services from public bodies, corporations, international organizations, and the government, promote the development of the digital economy and the information and communication technology sector, and help make domestic industry more competitive. The Indonesian government hopes to create a safer and more reliable environment for marketplace users with various efforts. Since the Personal Data Protection Law was passed, which focuses on general criteria for protecting personal data, any industry can use Personal Data Protection following its own needs. Among other things, the Personal Data Regulation seeks to safeguard and preserve citizens' fundamental rights, guarantee the public to get services, encourage digital economic growth, and support the improvement of domestic industry competitiveness.

Conclusions

Forms of legal protection efforts provided for consumer personal data leaks at Tokopedia and steps taken by Tokopedia in handling consumer personal data leaks. Being one of the biggest online retailers in Indonesia, Tokopedia has to protect customer privacy and adhere to legal requirements, including the ITE Law and Law Number 27 of 2022 concerning Personal Data Protection. When a data leak occurs, Tokopedia is responsible for informing users within 14 days and taking steps to secure its systems. Tokopedia also makes various efforts to improve security, such as encrypting passwords, appointing independent institutions for investigations, and conducting regular penetration tests. In addition, Tokopedia is committed to continue socializing to its users about the importance of personal data security measures, such as changing passwords regularly and maintaining the confidentiality of OTP codes. The research also highlights the importance of awareness of personal data privacy rights, in addition to the necessity of a robust legislative framework in this digital age to safeguard personal data. Customers are entitled to the privacy and security of their personal information. In the event of a hack, consumers are entitled to transparent information regarding the incident, including handling and mitigation efforts undertaken by Tokopedia. This protection should be guaranteed through a stricter and more comprehensive regulatory framework.

References

Achmad Thorik. 2023. Protection of Consumer Rights in the Use of E-Commerce: Perspective of Islamic Sharia Law. Tebuireng Journal of Islamic Studies and Society. Volume 04 No. 02.

Aldo Sonjaya. 2022. Legal Protection for Victims of Personal Data Leakage of Tokopedia Application Users based on Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Transactions. Bandung: Journal of Bandung Conference series: Law Studies Volume 2 Number 1.

Alice Kalagi, "The Position and Binding Force of Internet Transaction Agreements (Ecommerce)", Journal of Lex Privatum, Vol. 3, No. 4, October 2015.

Deanne Destriani Firmansyah Putri. 2020. Efforts to Prevent Consumer Data Leakage Through the Ratification of the Personal Data Protection Ruu (Case Study of E-Commerce bhinneka.com). National Conference on Law Studies: Legal Development Towards A Digital Society Era.

Efendi, J., I. (2016). Normative and Empirical Legal Research Methods. Depok: Prenada Media.

Indriani Muin. 2023. Personal Data Protection in E-Commerce Platforms to Enhance Indonesia's Digital Economic Development. Vol.1, No.2.

Inosentius Samsul. 2004. Consumer Protection, Possible Application of Absolute Liability, Jakarta: University of Indonesia.

Intan Nur Rahmawati & Rukiyah Lubis, "Win-Win Solution for Consumer Disputes", (Yogyakarta: Medpress Digital, 2014).

Muhammad Fathur. 2020. Tokopedia's Responsibility for Leaking Consumer Personal Data. National Conference on Law Studies: Legal Development Towards A Digital Society Era. Volume 03 No. 04.

Shidarta, Indonesian Consumer Protection Law, Revised Edition, Jakarta: Grasindo, 2004.