Journal of Social Research
P-ISSN: 2827-9832
E-ISSN: 2828-335x
Vol. 4, No. 12, November 2025
http://ijsr.internationaljournallabs.com/index.php/ijsr

Legal Protection of Consumer Personal Data in Business in the Digital Era

Dian Arifin, Wiwik Sri Widiarty, Richard Marolop Nainggolan
Universitas Kristen Indonesia, Indonesia
Email: dianarifin700@gmail.com, wiwik.widiarty@gmail.com, richardmn88@gmail.com

ABSTRACT

The rapid digitalization of business transactions has increased the risks of personal data misuse, creating an urgent need for robust legal protection. Despite the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), implementation challenges persist, including weak oversight and low compliance awareness among digital businesses. This study aims to analyze the legal certainty provided by the PDP Law for consumers experiencing personal data breaches and identify effective legal protection mechanisms in digital business transactions. This normative legal research employs statute and conceptual approaches, analyzing secondary data from laws, regulations, court decisions, and legal literature. Data were examined through legal synchronization analysis to assess regulatory alignment and implementation gaps. The study finds that while the PDP Law establishes legal certainty through consumers' rights to compensation (Article 12) and data control (Articles 15–20), the Consumer Protection Law lacks specific personal data protection provisions. Implementation faces obstacles including the absence of an independent supervisory authority, fragmented oversight, and low digital literacy among consumers and businesses. The PDP Law provides a legal foundation for consumer protection, but its effectiveness is hampered by structural and institutional challenges. Comprehensive implementation requires strengthening supervisory institutions, enhancing regulatory synergy, and increasing stakeholder awareness to ensure meaningful protection of consumer personal data in digital business transactions.

Keywords: *Legal Protection, Personal Data, Digital Business.*

This article is licensed under CC BY-SA 4.0

INTRODUCTION

Today, computers, smartphones, and telecommunications networks have become essential human needs, marking the birth of the Digital Age (Suler, 2016). Computer technology, with its speed and precision in completing tasks, has reduced labor requirements, operational costs, and human error (Ajiga, Okeleke, Folorunsho, & Ezeigweneme, 2024). However, behind this convenience, significant risks arise when system errors or misuse of technology occur, potentially causing serious harm to users (Farkas & Hronyecz, 2024). This phenomenon is increasingly complex because such misuse is not always accidental but sometimes carried out with specific goals that harm others (Haslam, 2016).

The rapid development of information technology in the digital era has become a global characteristic, leading to the disappearance of national boundaries (borderless) (Hosen, 2023). Countries with advanced digital infrastructure enjoy significant benefits from this progress, while developing countries face challenges such as unequal access to information and the emergence of new forms of digital colonialism (Kwet, 2019). The global paradigm has shifted, with a country's strength and progress now measured by its ability to build a strong and secure information network (Lahneman, 2010). This situation demands that every country, including Indonesia, build robust digital infrastructure and implement a legal system that protects the public from the risk of data misuse (Marune & Hartanto, 2021).

Advances in information technology have had a significant impact on all aspects of life (Yamin, 2019). Sectors such as trade, education, healthcare, and government have been digitized through the concepts of e-commerce, e-education, e-health, and e-government (Ullah, Pinglu, Ullah, Abbas, & Khan, 2021). People's activities are increasingly dependent on the internet, search engines, social media, and mobile applications, which provide easy access to information and efficient transactions (Verhoef et al., 2017). However, behind this

convenience, digital transformation poses serious threats related to cybersecurity, data privacy, and consumer protection, which are not yet fully guaranteed.

Digital transformation has changed transaction patterns, making them faster, more efficient, and seamless across time and space (Bonnet & Westerman, 2021). However, new challenges have emerged in the form of weak standards for data security, privacy, and consumer protection (Corones & Davis, 2017). Cases of online fraud, personal data theft, and misuse of information are on the rise (Ansar et al., 2021). As the volume of personal data stored by digital platforms increases, the risk of data leaks and misuse also increases (Ahmad, 2023). Therefore, personal data security is a critical concern amidst the rapid development of a digital economy based on public trust (Juneja, Goswami, & Mondal, 2024).

According to Dhoni Martien in his book "Personal Data Legal Protection," advances in cloud computing technology have encouraged many companies and government agencies to utilize cloud storage to store user data, including sensitive and personal data. Cloud-based services are now used by various public applications such as BMKG Info, Mobile JKN, BPOM Mobile, Lapor!, Signal, and commercial platforms like Tokopedia, Shopee, and mobile banking services. While efficient, the use of these systems increases the risk of data breaches if not accompanied by adequate legal and technical protections.

Personal data breaches have become one of the most dangerous forms of cybercrime in the modern digital world (Soomro & Hussain, 2019) . Personal data now has high economic value and is a valuable asset for both individuals and corporations. Data leaks can cause material losses, reputational damage, psychological distress, and even a loss of public trust in digital services. Governments, businesses, and the public are required to work together to uphold the principles of security and responsibility in personal data management to create a safe and ethical digital ecosystem.

The phenomenon of personal data leaks in Indonesia demonstrates the weakness of the legal system for protecting consumer data. One major case occurred in 2021 when data on 279 million Indonesians, allegedly from the BPJS Kesehatan (Social Security Agency for Health), was leaked and traded online. This incident caused public unrest and prompted the government to expedite the enactment of regulations regarding personal data protection. Prior to the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), Indonesia lacked a comprehensive legal framework to regulate personal data management, resulting in a high risk of breaches due to weak oversight and low public awareness of the importance of data protection.

Previous research has explored various aspects of this issue (Pang & Ki, 2016). The research by Prayuti (2024) examined the dynamics of consumer legal protection in the digital era, focusing on e-commerce practices and identifying significant gaps in data protection within existing consumer law frameworks. Meanwhile, the research by Ardika (2025) conducted a legal review of personal data protection specifically in e-commerce contexts, analyzing cases of user data leaks and highlighting the jurisdictional challenges in addressing cross-border data violations. However, while these studies identified regulatory weaknesses, they were conducted prior to the full implementation of the PDP Law and thus could not fully analyze its effectiveness.

Furthermore, the research by Dewi and Darma (2018) investigated legal protection for online service providers, focusing more on the liability of platforms rather than proactive protection mechanisms for consumers themselves. Conversely, research by Volchkov (2013) provided a valuable international perspective on security governance frameworks, yet its application within the specific socio-legal context of Indonesia remained unexplored. This creates a clear knowledge gap: while previous research has identified the problem of data vulnerability and the initial regulatory response, a comprehensive analysis of the implementation synergy between the new PDP Law, the ITE Law, and the Consumer

Protection Law in providing concrete legal certainty and redress for consumers in digital business transactions is still lacking.

Although the Personal Data Protection Law has been passed, its implementation still faces various obstacles, such as the lack of an independent institution authorized to oversee its implementation and a lack of awareness among business actors in complying with the regulation. In fact, Article 28G paragraph (1) of the 1945 Constitution expressly guarantees the right of every citizen to protection of themselves, honor, and property from the threat of violations. The fact that Indonesia is among the top 10 countries with the highest data breach rates in the world demonstrates the weakness of the existing protection system. Departing from this condition, this study seeks to examine in depth the legal protection of consumer personal data in digital business transactions, focusing on the effectiveness of the implementation of Law Number 27 of 2022 and the responsibilities of the government and business actors in realizing legal certainty in the digital era. Therefore, this thesis is entitled "Legal Protection of Consumer Personal Data in Business in the Digital Era."

Based on the previously explained background, this study formulates two main problems: first, whether Law Number 27 of 2022 concerning Personal Data Protection has provided legal certainty for consumers who experience personal data breaches in digital business transactions; and second, what legal protection measures can be provided to consumers whose personal data is harmed by digital business transactions. The purpose of this research is to fill the gap in understanding regarding the application of legal theory in dealing with the phenomenon of public data leaks in the digital era, as well as to provide insight regarding the government's role in enforcing legal instruments passed through the Personal Data Protection Law (PDP Law). This study also aims to encourage the government to take more effective steps to address the rampant misuse of personal data, as well as to provide practical concepts and recommendations regarding legal liability for material losses experienced by consumers and business actors in the context of digital business. Specifically, this study aims to analyze the extent to which Law Number 27 of 2022 provides legal certainty for consumers who experience personal data breaches and outlines the legal protection measures available for consumers harmed by these breaches. This research is expected to provide theoretical benefits by contributing to the development of legal science, particularly in providing information and understanding regarding rules and procedures for protecting personal data to help the public avoid the threat of hacking in digital businesses. Practically, this research is expected to serve as study material for interested parties and provide solutions to various legal issues arising in personal data protection within the digital business sector. Furthermore, the results of this research are expected to provide academic benefits for the Master of Law Postgraduate Program at the Indonesian Christian University (UKI) as one form of fulfilling the requirements for obtaining a Master of Law degree.

METHOD

The research was a normative legal study (library legal research). Normative legal research focused on legal norms within a specific legal system, aiming to study, interpret, and examine various laws, regulations, legal doctrines, and relevant court decisions. Using this approach, researchers constructed legal arguments based on interpretations of existing legal norms to gain a deep understanding of the substance and meaning of legal provisions related to personal data protection. This study specifically analyzed the forms of legal liability of business actors and consumers in the digital business context based on Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).

Secondary data served as the primary source and were obtained through library research covering concepts, theories, doctrines, and relevant laws and regulations. According to Ronny Hanitijo Soemitro's classification, secondary data in legal research consist of three categories: primary, secondary, and tertiary legal materials. Primary materials include laws and regulations such as the ITE Law and the PDP Law, along with relevant court decisions. Secondary materials encompass law books, scientific journals, articles, theses, and prior research on consumer personal data protection in digital businesses. Tertiary materials include legal dictionaries, encyclopedias, and the Great Indonesian Dictionary, which clarified the legal terminology and concepts used in this study.

The approach applied was normative juridical, emphasizing the statute approach and the historical approach. The statute approach examined the appropriateness and effectiveness of applying positive law to the issue of personal data leaks in digital business. This approach was essential because Indonesia follows the principle of law on the books, meaning actions are unlawful only if regulations govern them. The historical approach traced the background of the Personal Data Protection Law's enactment and compared it with legal developments in countries with established data protection systems. Combining these approaches provided a comprehensive understanding of the position and implementation of personal data protection law in Indonesia.

Legal synchronization analysis assessed the alignment between regulations governing personal data protection. This analysis occurred at two levels: vertical synchronization examined alignment between laws and regulations of different hierarchies, such as the ITE Law, the PDP Law, and their implementing regulations; horizontal synchronization compared regulations of equal standing, such as the ITE Law and the PDP Law, to assess consistency and comprehensiveness regarding personal data protection. The study also included a legal comparison between Indonesia and other countries to understand global data protection standards and how Indonesia could align its regulations with international practices.

Data collection involved library research through reading, recording, and citing relevant legal materials from various sources, including laws and regulations, books, legal journals, scientific articles, and official documents. The data were analyzed qualitatively and normatively by describing, interpreting, and linking applicable legal norms to address the research problem. Qualitative analysis examined theories, doctrines, and expert opinions to identify legal principles applicable to consumer personal data protection, detect legal gaps, and provide recommendations for improvement.

This research was original in focusing on the legal protection of consumer personal data in digital businesses by examining the relationship between the ITE Law, the PDP Law, and the Consumer Protection Law. It emphasized the effectiveness of positive law in providing legal certainty for consumers harmed by personal data leaks, the legal responsibilities of business actors, and the government's role in enforcement. Besides legal norm analysis, the thesis reviewed various personal data leak cases in Indonesia and assessed protection efforts through institutions such as the Financial Services Authority (OJK), the Ministry of Communication and Digital, the Police, and the Courts. Finally, it evaluated legal sanctions for personal data protection violations under the ITE Law, the PDP Law, the Criminal Code, and the Consumer Protection Law as a basis for strengthening the national legal system to meet digital-era data protection challenges.

RESULTS AND DISCUSSION

Legal Certainty for Consumers Experiencing Personal Data Breaches in Digital Business Transactions Based on Law Number 27 of 2022 Concerning Personal Data Protection

Legal Regulations Regarding Personal Data Breaches Through Law Number 27 of 2022 concerning Personal Data Protection

The evolution of corporate law in the digital era presents significant challenges for legal systems in many countries, including Indonesia. The development of information technology, particularly in digital commerce and internet-based services, demands regulatory changes to more comprehensively protect consumer rights. In this context, consumer personal data is a crucial element in digital transactions, as it includes sensitive information such as names, addresses, and financial identities. Unauthorized exploitation of personal data is a serious issue that requires strict legislative oversight. Therefore, legal protection of consumer personal data is not only an ethical responsibility but also an urgent legal necessity to maintain public trust in the digital ecosystem.

As a strategic step to address these challenges, Indonesia passed Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). This regulation provides a strong legal basis for the public to protect their personal data and requires all data controllers, including companies, to maintain its security and confidentiality. Previously, Law No. 8 of 1999 concerning Consumer Protection did not specifically regulate aspects of personal data protection in the digital space. Therefore, the PDP Law was introduced to fill this legal gap and emphasize the responsibility of business actors to maintain the confidentiality of consumer information. With the enactment of the PDP Law, consumers now have a stronger legal position to demand accountability if their personal data is misused, thereby strengthening legal certainty in digital transactions.

In practice, the implementation of the Personal Data Protection Law still faces various obstacles, primarily due to low digital literacy among the public and a lack of understanding among companies regarding their obligations regarding personal data management. However, personal data such as names, identity numbers, addresses, and financial information can be exploited for illegal activities if not properly protected. Therefore, companies are required to obtain explicit consent from data owners before collecting, processing, or distributing such information. Furthermore, the public needs to be educated on how to maintain personal data security online. Strengthening law enforcement and oversight of digital business actors is also key to ensuring the effective implementation of the Personal Data Protection Law, rather than merely being declarative.

The Personal Data Protection Law explicitly affirms individuals' rights to their personal data. Article 1, number 2, defines personal data protection as a collective effort to protect data during the collection, storage, and utilization process. Meanwhile, Article 1, number 6, defines a Personal Data Subject as an individual who is the legal owner of their personal data. These rights are further elaborated in Articles 5 to 14, which include the right to obtain clarity regarding data use, update personal information, and correct data errors. Furthermore, Article 12, paragraph (1) grants data subjects the right to sue and seek compensation in the event of a violation. Furthermore, Articles 15 to 20 regulate the right to delete, limit, and control the processing of personal data. These provisions share similar principles with the General Data Protection Regulation (GDPR) in the European Union, although its implementation in Indonesia still requires improvement, particularly in terms of speed and reporting mechanisms for violations, which are not yet as stringent as the 72-hour requirement stipulated in the GDPR.

Legal Regulations for the Protection of Consumer Personal Data Based on Law Number 8 of 1999 concerning Consumer Protection

In today's digital business era, businesses offer a variety of products and services both directly and online, such as online loans, credit facilities, and digital insurance. However, this increase in business activity has also been accompanied by increasing public complaints regarding the leakage of consumers' personal data. Many cases indicate that individuals misuse personal information, such as telephone numbers, addresses, or financial data, without the owner's consent. This situation creates a sense of insecurity and discomfort for consumers

whose rights should be protected by law. Based on Law Number 8 of 1999 concerning Consumer Protection, Article 1 point (3) defines a business actor as an individual or legal entity that conducts business activities within the jurisdiction of Indonesia, either alone or together, in various economic sectors. Therefore, every digital business actor has a legal obligation to maintain the confidentiality of its consumers' personal data in every transaction.

The relationship between business actors and consumers is closely related to the utilization of products and services. In this context, Article 1 points (4) and (5) of the Consumer Protection Law defines "goods" as including tangible and intangible objects used for the benefit of consumers, while "services" include services provided for the benefit of the public. Therefore, consumers in the digital era are positioned as subjects who must be protected by law. As expressed by Lowe, Consumer Protection Law is a rule of law that recognizes the bargaining weakness of the individual consumer and ensures that weakness is not unfairly exploited — that consumer protection law exists to prevent exploitation of the weak bargaining position of consumers. Thus, the Consumer Protection Law is a fundamental instrument in ensuring fairness and balance between business actors and consumers, especially in the context of electronic transactions and personal data protection.

Furthermore, attention to consumer protection has also become a global agenda. United Nations Resolution Number 39/248 of 1995 concerning Guidelines for Consumer Protection affirms six basic principles of consumer protection, namely: (1) protecting consumers from dangers to health and safety, (2) guaranteeing consumers' socio-economic interests, (3) ensuring the availability of adequate information, (4) providing consumer education, (5) providing effective redress mechanisms, and (6) providing the freedom to form consumer organizations. Indonesia, through Law Number 8 of 1999, has adopted some of these principles in Article 4, which grants consumers the right to comfort, security, and safety in using goods or services. In the digital context, this provision can be interpreted as protecting the privacy and security of consumers' personal data. Meanwhile, Article 7 regulates the obligations of business actors to act in good faith, maintain the confidentiality of consumer data, and not misuse it for unauthorized commercial purposes.

Furthermore, several articles in the Consumer Protection Law are directly related to personal data protection, including Article 4 (the right to accurate and honest information), Article 7 (the obligation of business actors to provide clarity regarding the use of personal data), Article 8 (prohibition of actions that harm consumers, including data misuse), Article 13 (responsibility for losses resulting from violations of consumer rights), and Article 19 (administrative and criminal sanctions for business actors who violate). These provisions demonstrate that although the Consumer Protection Law does not explicitly mention “personal data,” the substance of its protection still covers this aspect. The main objective of this law is to create a protection system that guarantees legal certainty, awareness, and responsibility of business actors, as stipulated in Article 3. In addition, Article 1366 of the Civil Code emphasizes the principle of liability for losses resulting from negligence or unlawful acts. Thus, business actors who neglect to protect consumers' personal data can be subject to legal liability, either through civil lawsuits or administrative sanctions from the Consumer Dispute Resolution Agency (BPSK), a concrete form of legal protection in the digital era.

Challenges in Facing Personal Data Protection

In Indonesia, law enforcement efforts to prevent consent violations in consumer protection practices in the digital era still face various institutional, cultural, and structural barriers. Despite the enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) as a comprehensive legal framework, its implementation in the field has not been optimal. These obstacles stem not only from formal legal aspects, but also from institutional preparedness, inter-regulatory coordination, technical limitations, and low public

awareness of privacy rights. As a result, even though legal standards are in place, their effectiveness in protecting consumers in the digital world remains far from expectations.

One of the main obstacles was the fragmentation of regulations before the enactment of the Personal Data Protection Law. Previously, data protection aspects were regulated scattered across the Electronic Information and Transactions (ITE) Law, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and sectoral regulations in banking, telecommunications, and healthcare. These norms often overlapped and even contradicted, causing confusion for businesses and law enforcement officials in determining compliance obligations. Harmonization between regulations remains a major obstacle because not all sectoral regulations have been updated to align with the Personal Data Protection Law. As a result, inter-agency coordination in addressing personal data breaches was often slow and ineffective, reducing the effectiveness of legal protection for digital consumers.

Furthermore, institutional capacity and oversight remain weak. The Data Protection and Data Protection Law mandates the establishment of an independent data protection authority tasked with monitoring, receiving complaints, and imposing sanctions for violations. However, as of 2025, this agency is still under development, leaving oversight duties scattered across various agencies without strong coordination. The limited human resources with the competence to serve as Data Protection Officers (DPOs) further exacerbate the situation. Many digital businesses lack dedicated staff to ensure compliance with data protection principles. As a result, data collection and processing practices often lack a clear legal basis, opening up opportunities for misuse of personal information.

Another obstacle arises from low public awareness of the right to personal data. Many people, particularly in rural areas, do not yet understand that they have the right to refuse to provide personal data to third parties without a valid reason. As a result, data such as addresses, telephone numbers, and even financial information is often readily provided to digital platforms without considering the risks. This situation is exploited by unscrupulous business actors who manipulate or sell data for economic gain. Meanwhile, law enforcement officials also face difficulties in handling data breach cases due to limited digital forensic capabilities, tracking infrastructure, and electronic evidence tools. Digital traces such as system logs and metadata are often deleted by perpetrators, making the process of proving data in court complex and time-consuming.

At the global level, cross-border law enforcement challenges further complicate the situation. Much of Indonesian citizens' personal data is stored by foreign companies or on overseas servers outside national jurisdiction. This makes it difficult for authorities to prosecute violations committed by international corporations. Addressing this challenge requires stronger international cooperation in the areas of information exchange, data security standards, and cross-border sanctions enforcement. Furthermore, domestic challenges such as a lack of cybersecurity infrastructure, the lack of strict sanctions, and weak inter-agency coordination further undermine digital consumer protection. Therefore, the mere existence of laws is not enough; systematic action is needed, including institutional strengthening, increased digital literacy, and investment in data security, to ensure effective law enforcement and protect consumers' privacy rights in the increasingly complex digital economy.

Legal Certainty for Consumers Experiencing Personal Data Breaches in Digital Business Transactions Based on Law Number 27 of 2022 Concerning Personal Data Protection

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) was enacted in response to the increasing number of digital business activities and consumer personal data breaches in Indonesia. This regulation affirms the principle of legal certainty, as emphasized by Satjipto Rahardjo, that the law must provide real and impartial protection, especially for

vulnerable legal subjects such as consumers in the digital era. Through the PDP Law, personal data protection is recognized as a constitutionally guaranteed human right, providing a strong legal basis for every individual to ensure that their right to privacy and control over their personal data is not violated. This law also places strict obligations on data controllers to maintain the security of consumer data, process data legally, and be fully responsible for any violations that occur. Thus, the PDP Law creates legal certainty that protects consumers from arbitrary digital business practices.

In practice, the Personal Data Protection Law requires digital businesses to act transparently and obtain explicit consent from consumers before processing personal data. Data controllers must disclose the purpose of data collection, scope of use, retention period, and consumers' rights over their data. Consumers are given the legal right to access, correct, delete, or withdraw consent to the use of their personal data through clear and measurable mechanisms. This provision affirms consumers' position as active legal subjects with control over their personal data, not merely objects in a digital system. In this context, the law is not only declarative but also operational, as it provides concrete rights that can be enforced before the law in the event of a violation.

The Data Protection and Privacy Law also strengthens legal certainty by providing administrative and criminal sanctions for businesses that violate data protection provisions. These sanctions can include written warnings, temporary suspension of data processing activities, substantial administrative fines, and even imprisonment for those who intentionally disseminate data without permission. The strictness of these sanctions demonstrates the state's efforts to create a deterrent effect for digital businesses while simultaneously providing a sense of security for consumers. In the context of civil law, violations of the obligation to maintain data confidentiality can be sued under Articles 1365 and 1367 of the Civil Code concerning unlawful acts and liability for losses to others. Thus, the Indonesian legal system provides a clear redress mechanism for consumers harmed by the leak or misuse of personal data.

However, while the Personal Data Protection Law provides a robust legal framework, significant challenges remain to its implementation and enforcement. Many digital businesses do not fully understand their legal obligations, while consumers are often unaware of their rights to their personal data. Low digital literacy, weak oversight, and the non-optimal functioning of independent supervisory authorities are key obstacles. Furthermore, Indonesia's cybersecurity infrastructure remains weak, resulting in frequent data breaches on major platforms like Tokopedia and government agencies. This demonstrates that the principle of legal certainty promised by the Personal Data Protection Law has not been fully realized in practice. Therefore, for the law to truly provide certainty and justice, synergy is needed between the government, businesses, and the public through increased digital literacy, consistent law enforcement, and strict oversight of personal data management.

Examples of Cases of Personal Data Protection Violations

1. **Data Leak Cases from Online Services**

   Data breaches are the first step in the most common theft of personal information. Users of financial applications such as banks, PayLater, e-commerce, or multi-purpose payment systems are the most frequent victims of data breaches. Data leaks caused by hackers have been reported numerous times. People discover that the applications they use have leaked their personal information, including names, ID numbers, phone numbers, addresses, and other contact details. Typically, hackers upload this information to websites for interested parties to purchase. This data is then exploited for various fraudulent purposes.

2. Identity Leakage Through Phishing

This method is carried out by users receiving communications via WhatsApp, SMS, or email that appear to come from a trusted source, such as the victim's bank account. For example, when lottery winners are announced, the message is usually very credible, as if it were from a financial institution. Victims provide account details and other sensitive information to the fraudster because they trust them. The fraudsters exploit the victim's bank account to obtain their personal information, which they inadvertently provide. This method is very simple and dangerous, because by clicking on the domain/URL provided by the fraudster to the victim, the victim's personal data can immediately be exploited by the perpetrator. Typically, a link is included in the message received via WhatsApp or other social media. For more information, the victim is directed to click on the page. This link turns out to be a way for hackers to obtain the victim's personal data on their phone when clicked.

3. Data Theft Cases from Technology Companies

A data breach involving a technology company is a series of events in which personal or sensitive data is illegally accessed, stolen, or hacked by unauthorized individuals. This can include the theft of hardware, including laptops or servers storing critical data, unauthorized access to computer systems, or attacks on company data. Customer information, financial data, trade secrets that may provide a business with a key competitive advantage, product designs, and application source code are some examples of company data that are vulnerable to theft. Data theft by a technology company can have far-reaching consequences, including financial losses due to the erosion of client trust, data and system recovery costs, and potential fines from regulatory agencies if customer data is compromised.

4. Wiretapping or Illegal Access and Personal Data Without Rights

The Jakarta Metropolitan Police's Cyber Investigation Directorate uncovered a case of illegal access to personal data at a shipping company from December 2024 to January 2025. The case began around December 2024 and continued until January 2025, when approximately 100 customer complaints were received regarding online purchases from TikTok. These purchases were delivered through Ninja Xpress, with a Cash On Delivery (COD) payment method. Ninja Xpress then conducted an audit to determine the number of packages received before the specified time for the COD payment method. COD payment methods have a 7-day delivery time.

The results of the audit found that there were 294 shipments with COD payment types that were completed faster than seven days. "This was due to the abuse of authority by Ninja Xpress employees at the Lengkong office, Bandung, West Java. Ninja Xpress uses the OpV2 system where the NJVT receipt (secret code) containing shipping information for customer purchases from the e-commerce is protected. However, there were unscrupulous Ninja Xpress employees who accessed the OpV2 system and opened protected customer data with the term "unmasking". The customer data included the name of the orderer, the number of orders, the type of order, the delivery address, the orderer's mobile phone number and the COD order fee. The data was then sold to an external party who then came to the "customer" with a fake package, and received COD payments, namely shipping costs and the price of the goods purchased by the "customer".

Ninja Xpress (seller) suffered material losses of around Rp35.2 million and immaterial losses in the form of loss of trust from Tiktok Shop and the public. The perpetrators were successfully arrested on Monday, May 5, 2025, for suspect T was

arrested in Bandung. While MFB was arrested in Cirebon. The suspects were charged with Article 46 Jo. Article 30 of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions or Article 48 Jo. Article 32 of Law Number 11 of 2008 as Last Amended by Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

5. **The Case of Selling ID Card Data and Selfie Photos on Twitter**

The Indonesian National Police (Polri) is investigating reports of ID card data and selfies being sold on Twitter. The sale of ID card data and selfies belonging to other people on Twitter has alarmed netizens and the general public. The owners of the uploaded ID card and selfie are unknown. However, the caption reads: "Ready HD selfie ID card, if interested, just PM me if it's still fresh." Cases of personal data leaks have recently become increasingly common.

Legal Protection Efforts for Consumers Whose Personal Data is Harmed by Digital Business Transactions

Legal Protection Efforts Through the Financial Services Authority

The implementation of Law Number 21 of 2011 concerning the Financial Services Authority (hereinafter referred to as the OJK Law) is expected to strengthen protection of customer financial privacy and oversee digital business activities in the financial services sector. This law emphasizes that customers of financial institutions are legal subjects who must be protected because they act as parties who carry out digital trading activities and other financial transactions. Chapter VI of the OJK Law emphasizes the institution's responsibility in providing protection to consumers and the public, which is implemented through the authority to stipulate Financial Services Authority Regulations (POJK). Based on Article 31 of the OJK Law, POJK functions as additional implementing regulations to ensure legal protection for consumers in the financial services sector. One important regulatory product is POJK Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector, which serves as a concrete foundation for implementing consumer protection principles in the financial industry.

The establishment of the Financial Services Authority (OJK) is mandated by Article 34 of Law Number 3 of 2004 concerning Amendments to Law Number 23 of 1999 concerning Bank Indonesia, which requires the establishment of an independent regulatory body in the financial services sector. The establishment of this body is inseparable from the experience of the 1997 Asian financial crisis, which revealed the weakness of banking supervision and the need for a stronger, independent authority free from political intervention. The trend of establishing similar institutions also occurred in various countries such as the United Kingdom (1997), Germany (1949), and Japan (1998). In response to these dynamics, the Indonesian government finally established the Financial Services Authority through Law Number 21 of 2011, which was promulgated in November 2011, with the aim of adopting international best practices in transparent, independent, and accountable supervision of financial institutions.

The Financial Services Authority (OJK) was established as an independent institution with two primary functions: regulation and supervision of all activities in the financial services sector. Based on Articles 6, 8, and 9 of the OJK Law, this institution has dual jurisdiction, including the authority to formulate regulations and oversee the implementation of activities of financial services institutions such as banking, insurance, pension funds, capital markets, financing institutions, and digital financial service providers. The main objectives of the OJK's establishment are stated in Article 4, namely to ensure that all business activities in the financial

services sector run in an orderly, fair, transparent, and responsible manner; to be able to realize a stable and sustainable financial system; and to protect the interests of the public and consumers. Thus, consumer protection is an integral function of the OJK's existence, in line with the mandate of Law Number 8 of 1999 concerning Consumer Protection (UUPK).

The relationship between the OJK Law and the Consumer Protection Law can be seen from the aspect of their shared objectives, namely ensuring legal certainty and justice for the community. Although the OJK Law is not a regulation that directly regulates consumer protection, its substance closely intersects with the UUPK because it contains the principle of protection for customers as users of financial services. This is emphasized in the considerations section of the OJK Law, letter (a), which states that activities in the financial services sector must be able to protect the interests of consumers and the community. In addition, Article 1 number (15) defines consumers as parties who place funds or utilize services in financial services institutions such as banking, insurance, and pension funds. Thus, the concept of "consumer" in the OJK Law has a more specific scope than the UUPK, which defines consumers more broadly as users of goods and/or services in all sectors of economic life.

As a concrete form of consumer protection, the Financial Services Authority (OJK) has issued several implementing regulations that strengthen the supervisory and dispute resolution functions of consumers in the financial services sector. These regulations include OJK Regulation Number 18/POJK.07/2018 concerning Consumer Complaints Services in the Financial Services Sector, OJK Regulation Number 61/POJK.07/2020 concerning Alternative Dispute Resolution Institutions (LAPS) in the Financial Services Sector, and OJK Regulation Number 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector. Through these regulations, the OJK emphasizes the complaint, handling, and dispute resolution mechanisms between consumers and financial services providers (PUJK). The dispute resolution process can be carried out in stages, starting from receiving and handling complaints to out-of-court settlement through LAPS. Financial services providers are also required to resolve complaints in writing within a maximum of 20 business days and are prohibited from charging consumers complaint service fees.

Thus, the implementation of Law Number 21 of 2011 concerning the Financial Services Authority (OJK) and its derivative regulations demonstrates the Indonesian government's commitment to strengthening legal protection for consumers in the financial services sector, including in the context of digital businesses. The OJK acts as an independent supervisor, ensuring that financial services businesses conduct their business activities transparently, fairly, and accountably, and provides an effective dispute resolution mechanism outside the courts. However, increased synergy between the OJK, the Ministry of Communication and Digital, and other law enforcement agencies is still needed to strengthen the protection of personal data of customers and users of digital financial services. This is crucial to ensure that regulatory implementation is effective and truly provides legal certainty, justice, and a sense of security for the public as consumers in the era of digital economic transformation.

Consumer Protection Efforts Through the Ministry of Communication and Digital

The government, through the Ministry of Communication and Digital (Komdigi) and the Ministry of Trade, continues to strive to strengthen consumer protection systems in the digital era. Through the Directorate of Consumer Empowerment within the Directorate General of Consumer Protection and Trade Order (Ditjen PKTN), the "Smart and Empowered Consumers in the Digital Era" program continues to be promoted as a form of public education to ensure they understand their rights and obligations in digital commerce activities. One concrete step taken is the implementation of consumer protection training, which aims to increase public understanding of consumer rights, promote information transparency, and foster a culture of critical thinking in every digital transaction. Consumers who understand their

rights, are able to demand transparency of information about goods or services, and can make wise decisions are classified as smart and empowered consumers.

As a concrete form of legal protection for consumers in the digital commerce sector, the government issued Government Regulation Number 80 of 2019 concerning Electronic Commerce (E-Commerce). This regulation serves as a crucial legal basis for regulating online transactions, the legal relationship between businesses and consumers, and dispute resolution mechanisms in e-commerce. One of the primary obligations stipulated in this regulation is the provision of consumer complaint services by digital businesses. Furthermore, Article 2 of Government Regulation 80/2019 establishes a broad scope of regulation, encompassing aspects of business actors, E-Commerce implementation, electronic contracts, personal data protection, and guidance and supervision. Thus, this regulation serves as a national legal umbrella to ensure that digital business practices are conducted fairly, transparently, and oriented towards consumer interests.

One important aspect of Government Regulation Number 80 of 2019 is the regulation regarding electronic contracts as stipulated in Chapter X Articles 50 to 57. Electronic contracts are considered valid and binding if they meet the provisions of Article 52, namely the existence of an agreement between the parties, legal capacity, clarity of the object of the transaction, and not contrary to law and morality. In addition, Article 53 emphasizes that electronic contracts must contain minimal information such as the identity of the parties, specifications of goods or services, transaction value, payment terms, delivery mechanisms, and return procedures. On the other hand, Article 53 paragraph (2) prohibits the inclusion of standard clauses that are detrimental to consumers, namely unilateral provisions that limit consumer rights or impose unfair responsibilities. This prohibition is in line with the principle of consumer protection as stipulated in Law Number 8 of 1999, which emphasizes a balanced relationship between business actors and consumers in every transaction.

The provisions in Article 53 reflect the principle of transparency and responsibility of business actors in providing complete and honest information to consumers. This transparency is a crucial foundation for preventing contractual misunderstandings and increasing public trust in e-commerce platforms. Furthermore, the regulation prohibiting standard clauses serves to protect consumers from the practice of exploiting unilateral contracts often carried out by businesses with a stronger bargaining position. Thus, this regulation not only provides legal certainty for both parties but also upholds the principles of fairness and balance in contractual relationships. This principle is highly relevant to the development of the digital economy, which demands protection for users of increasingly broad and complex online services.

Furthermore, Article 57 of Government Regulation Number 80 of 2019 regulates the responsibility of business actors for technical errors in electronic systems. Based on this provision, if a technical error occurs due to an unsafe or unreliable system, the electronic contract is automatically null and void. In such circumstances, consumers are not obliged to return the goods or services received, and all losses are the responsibility of the business actor. This provision is a form of preventive and repressive legal protection for consumers, and encourages business actors to ensure that the electronic systems they use are safe, responsible, and meet standards. This principle emphasizes that business actors are obliged to guarantee the security of their digital systems, because negligence in technical aspects can result in legal consequences and losses for consumers.

In addition to contractual protection, Government Regulation Number 80 of 2019 also regulates the protection of personal data in Chapter XI, Articles 58 to 62. Article 59 emphasizes that personal data must be obtained legally, used only for clear purposes, maintained for accuracy, and protected by an adequate security system. Data owners even have the right to request the deletion of all their personal data if they stop using digital services. Furthermore, Article 80 regulates administrative sanctions for businesses that violate consumer protection

provisions, ranging from written warnings, priority watchlists, blacklists, service blocking, to revocation of business licenses. These sanctions emphasize the state's position in providing effective and equitable legal protection for the public in the era of digital commerce. Overall, Government Regulation Number 80 of 2019 plays a crucial role in building a safe, transparent, and consumer-oriented digital business ecosystem as an integral part of national economic transformation.

Legal Efforts to Protect Consumers Through the Police

For consumers who suffer losses due to the actions of business actors who do not comply with legal provisions, Risma Dewi Hermawan et al. stated that consumers have the right to file a complaint with the Indonesian National Police. Several requirements that must be met include: being an Indonesian citizen, bringing proof of a bank statement, making a complaint letter, and an official statement. After the report is received, the police are required to follow up in accordance with Article 5 of the Criminal Procedure Code (KUHAP), which stipulates that investigators are required to receive and examine reports or complaints from the public. Based on Article 1 number 4 of the KUHAP, investigators are tasked with searching for and finding an event suspected of being a crime to determine whether an investigation is necessary. In this case, the police are tasked with collecting evidence and identifying the perpetrator so that legal proceedings can be carried out in accordance with applicable provisions as stipulated in Article 1 number 2 of the KUHAP.

The next stage in the legal process is the investigation, as stipulated in Regulation of the Chief of the Indonesian National Police (Perkap) Number 14 of 2012 concerning the Management of Criminal Investigations. Based on Article 4 of the Perkap, the basis for initiating an investigation includes a police report or complaint, a task order, an investigation report, an investigation warrant, and a notification letter for the commencement of an investigation. Furthermore, Article 1 number 21 of Perkap 14/2012 states that a police report accompanied by one credible piece of evidence is considered sufficient initial evidence to arrest a party suspected of committing a crime. This provision is reinforced by Article 184 of the Criminal Procedure Code, which stipulates that valid evidence in a criminal case includes witness testimony, expert testimony, letters, clues, and the suspect's statement. This investigative stage is crucial for building a strong legal basis before the case is handed over to the prosecutor's office for prosecution.

In addition to these legal measures, the Indonesian National Police (Polri) also issued a preventive appeal to the public to prevent them from easily becoming victims of fraud or crime in digital businesses. The public is advised not to click on suspicious links or contact unknown numbers sent via SMS or messaging applications such as WhatsApp. If they encounter any indication of digital fraud, the public can verify the number and report it through the official website https://patrolisiber.id or via email info@cyber.polri.go.id. Furthermore, the public can also report cases to the Investment Alert Task Force (SWI) via email waspadainvestasi@ojk.go.id, and report dangerous or detrimental content via aduankonten@kominfo.go.id. These steps are a form of preventive legal protection so that the public can be more vigilant, digitally protected, and empowered in facing the risks of cybercrime and business practices that harm consumers.

Legal Protection Efforts Through the Courts

With the rapid growth of social media and the internet, the issue of protecting consumers' personal data has become increasingly crucial. Information such as names, addresses, telephone numbers, and other personal data collected by various digital platforms now has high economic value and is often exploited for business and marketing purposes. Although this data collection is generally conducted legally, there is still the potential for

misuse that can harm consumers. In a legal context, protecting personal data includes efforts to guarantee the rights of legal subjects as stipulated in laws and regulations. Legal protection can be divided into two types: preventive and repressive, each of which serves to prevent and prosecute violations of individual rights, including consumers, in the digital realm.

According to Muchsin, preventive legal protection is provided to prevent or stop legal violations before losses occur. This protection is implemented through regulatory mechanisms in laws that provide legal subjects with the opportunity to submit objections before a government decision becomes legally binding. The goal of preventive legal protection is to prevent conflicts or disputes, while simultaneously encouraging caution among government and business actors in acting to avoid harming the public. This form of protection is important in the digital context because it provides space for consumers to take preventative action before their rights are violated, particularly in the management of personal data by online service providers. Thus, preventive legal protection serves as an initial safeguard to avoid practices that violate consumers' rights to privacy and data security.

Meanwhile, repressive legal protection functions as a form of law enforcement when a violation has occurred. According to CST Kansil, repressive protection is realized through the application of sanctions, such as fines, criminal penalties, or civil lawsuits, aimed at resolving disputes between consumers and business actors. In Indonesia, this form of repressive protection is reflected in Article 45 of Law Number 8 of 1999 concerning Consumer Protection, which grants every aggrieved consumer the right to sue a business actor through a dispute resolution institution or a general court. This article serves as the primary legal basis for consumers to fight for their rights when experiencing losses due to digital transactions or personal data breaches. Thus, the Consumer Protection Law serves as a fundamental legal instrument in upholding justice for consumers, whose implementation is interconnected with the Personal Data Protection Law (Law No. 27 of 2022) and the Electronic Information and Transactions Law (ITE Law) as a unified legal protection system in the digital era.

Legal Sanctions for Violations of Consumer Personal Data Protection

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) regulates the implementation of electronic systems and digital transactions, including the protection of personal data. This regulation emphasizes that violations of personal data protection provisions can be subject to administrative and criminal sanctions, ranging from fines to imprisonment. This provision aims to create a sense of security, trust, and legal certainty in digital activities. For example, Article 26 emphasizes that the use of personal data in the digital space must be accompanied by the consent of the data owner. If this right is violated, the data owner has the right to file a lawsuit for losses suffered. In addition, electronic system organizers (PSE) are required to provide a mechanism for deleting personal data upon individual request or based on a court decision. Meanwhile, Article 30 paragraph (3) and Article 32 prohibit the illegal and unauthorized dissemination of personal data, with strict criminal penalties, as a form of repressive protection against the misuse of personal data in digital activities.

Furthermore, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is a major milestone in the legal framework for data protection in Indonesia. This law regulates administrative and criminal sanctions for violations of unauthorized personal data management, as stipulated in Articles 66 to 69, including fines of up to tens of billions of rupiah and imprisonment for serious violations. Furthermore, Articles 37 to 42 stipulate the obligation for data controllers to maintain the security of personal data and provide data subjects with rights, such as the right to access, correct, or delete their personal data. The PDP Law complements the ITE Law by specifically emphasizing the governance and accountability of

digital business actors regarding consumer personal data, while strengthening legal certainty in the increasingly complex era of digital transformation.

In the Criminal Code (KUHP), the protection of personal privacy is regulated by Article 322, which prohibits the disclosure of secrets that could harm another party. However, this provision is more relevant in the context of certain positions or professions, rather than in the context of personal data protection in the digital era. Therefore, this article is considered inadequate as the primary legal basis for addressing the challenges of modern personal data breaches. The role of the KUHP has now been replaced by legal instruments that are more contextual and adaptive to developments in information technology, namely the ITE Law, the PDP Law, and the Consumer Protection Law, which synergistically protect individual rights against misuse of personal data in digital transactions and online business activities.

In addition, Law Number 8 of 1999 concerning Consumer Protection (UUPK) also provides a legal basis for the protection of consumers' personal data. Article 4 paragraph (1) letter e affirms the consumer's right to obtain protection for security and safety in the use of goods and/or services, including protection of personal data. Furthermore, Article 18 requires business actors to maintain the confidentiality of consumer data and ensure the security of the information they manage. If a business actor violates this provision, Articles 62 to 65 stipulate administrative and criminal sanctions as a form of repressive legal protection. Thus, the UUPK serves as an important foundation that complements the ITE Law and the PDP Law, ensuring that digital consumers have strong rights to the security of their personal data and guarantees of justice in the event of violations by business actors in the digital era.

CONCLUSION

Law Number 27 of 2022 on Personal Data Protection provides legal certainty for consumers in digital business transactions by granting rights such as suing for compensation and controlling personal data processing, while the Consumer Protection Law offers only general protection without specific personal data provisions. Government enforcement efforts involve oversight by the Financial Services Authority (OJK), consumer education, and transparency requirements for businesses, but challenges like weak supervision, the lack of an independent data protection authority, low awareness, and fragmented regulations limit effective protection. Future research could investigate strategies to strengthen regulatory coordination and develop a robust data protection authority to improve enforcement and public awareness in Indonesia’s digital economy.

REFERENCES

Ajiga, D., Okeleke, P.. A., Folorunsho, S. O., & Ezeigweneme, C.. (2024). The role of software automation in improving industrial operations and efficiency. International Journal of Engineering Research Updates, 7(1), 22–35.

Ansar, S.. A., Yadav, J., Dwivedi, S.. K., Pandey, A., Srivastava, S.. P., Ishrat, M., Khan, M.. W., Pandey, D., & Khan, R.. A. (2021). A critical analysis of fraud cases on the Internet. Turkish Journal of Computer and Mathematics Education, 12(12), 2164–2186.

Ahmad, Nehaluddin. (2023). Data privacy issues and risks with sharing on social media: An inquiry. *Russian Law Journal*, *11*(4), 597–611.

Bonnet, D., & Westerman, G.. (2021). The new elements of digital transformation. MIT Sloan Management Review, 62(2), 82–89.

Corones, S., & Davis, J.. (2017). Protecting consumer privacy and data security: Regulatory challenges and potential future directions. Federal Law Review, 45(1), 65–95.

Farkas, T., & Hronyecz, E.. (2024). The Risks and Danger of Smart Devices Exposing Personal Information: Dark Side of Convenience. In 2024 IEEE 22nd Jubilee International Symposium on Intelligent Systems and Informatics (SISY) (pp. 39–44). IEEE.

Hosen, B.. (2023). Navigating the borderless horizon: A review study of challenges & opportunities of borderless world. International Journal of Research on Social and Natural Sciences, 8(2), 33–41.

Haslam, Nick. (2016). Concept creep: Psychology's expanding concepts of harm and pathology. *Psychological Inquiry*, *27*(1), 1–17.

Juneja, A., Goswami, S.. S., & Mondal, S.. (2024). Cyber security and digital economy: opportunities, growth and challenges. Journal of Technology Innovations and Energy, 3(2), 1–22.

Kwet, M.. (2019). Digital colonialism: US empire and the new imperialism in the Global South. Race & Class, 60(4), 3–26.

Lahneman, W.. J. (2010). The need for a new intelligence paradigm. International Journal of Intelligence and CounterIntelligence, 23(2), 201–225.

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

Ronny Hanitijo Soemitro. (1994). Legal Research Methodology and Jurimetry. Ghalia Indonesia.

Marune, A.. E.. M., & Hartanto, B.. (2021). Strengthening personal data protection, cyber security, and improving public awareness in Indonesia: Progressive legal perspective. International Journal of Business, Economics, and Social Development, 2(4), 143–152.

Pang, M.. F., & Ki, W.. W. (2016). Revisiting the idea of "critical aspects." Scandinavian Journal of Educational Research, 60(3), 323–336.

Soomro, T.. R., & Hussain, M.. (2019). Social media-related cybercrimes and techniques for their prevention. Applied Computer Systems, 24(1), 9–17.

Suler, J.. R. (2016). Psychology of the digital age: Humans become electric. Cambridge University Press.

Ullah, A., Pinglu, C., Ullah, S., Abbas, H.. S.. M., & Khan, S.. (2021). The role of e-governance in combating COVID-19 and promoting sustainable development: A comparative study of China and Pakistan. Chinese Political Science Review, 6(1), 86–118.

Verhoef, P.. C., Stephen, A.. T., Kannan, P.. K., Luo, X., Abhishek, V., Andrews, M., Bart, Y., Datta, H., Fong, N., & Hoffman, D.. L. (2017). Consumer connectivity in a complex, technology-enabled, and mobile-oriented world with smart products. Journal of Interactive Marketing, 40(1), 1–8.

Yamin, M.. (2019). Information technologies of 21st century and their impact on the society. International Journal of Information Technology, 11(4), 759–766.