Jurnal Sakato Ekasakti Law Review
e-ISSN: 2829-0305 | p-ISSN: 2829-1298
Volume 5, Issue 1, April 2026
Website: https://journal.unespadang.ac.id/JSELR

Civil Liability Digital Platform Regarding Personal Data Leaks Following the Enactment of Law Number 27 of 2022 Concerning Personal Data Protection

Ulfanora [(1)]*, Nanda Utama [(1)]
[(1)] Faculty of Law, Universitas Andalas, Padang, Indonesia

*Corresponding author's e-mail: ulfanorananda@gmail.com

Article Info
Revised: 2026-05-16
Accepted: 2026-06-18
Published: 2026-06-25

Keywords:
Personal Data; Data Leakage; Civil Liability

Abstract
The rapid development of technology has impacted various aspects of life, including economic, social, cultural, legal, and political aspects. This technological advancement has transformed the way people communicate and the provision of government services to the public. Information technology has become a new way for people to obtain information autonomously. Technology has become a Human Right to Digital Access. In general, the public is not yet aware of the impact of information misuse, resulting in low awareness of personal data protection. As a form of government concern for the public, who are both users and actors in this digital development, various regulations or rules have been established to provide legal protection for all people in utilizing the currently rapidly developing digital advancements. The existence of Law Number 27 of 2022 concerning Personal Data Protection is due to the numerous cases of data leaks in Indonesia. Research results explain thatFirst, Indonesia has ratified personal data protection regulations since 2022. The ratification of personal data protection regulations is effective starting from 2024. When Law Number 27 of 2022 concerning personal data protection was ratified into regulations and implemented in society, there were still shortcomings that became obstacles in its implementation in society. Second, Following the enactment of Law Number 27 of 2022 concerning Personal Data Protection, the civil liability of digital platforms has provided legal certainty. Law Number 27 of 2022 concerning Personal Data Protection explicitly places the burden of responsibility on them as data controllers. If a leak occurs due to a security system failure, they can no longer avoid legal responsibility to compensate for the losses you have suffered as a data subject.

INTRODUCTION

Indonesia adheres to the concept of a state based on law with a legal system *rule of law*[1]. The concept adopted by the Indonesian state not only regulates governmental power but also assists the government in regulating society, particularly its behavior as a nation. To achieve the noble goal of improving public welfare, the government must be firm and prevent it from falling under the control of any party seeking to exploit that power for personal or group interests.

As a nation that adheres to the concept of law, specifically ensuring equitable public welfare, the government needs to provide legal protection to all citizens. This legal protection involves establishing regulations and sanctions for violators to provide a deterrent effect. The law, in its process, prohibits all elements of society from complying with applicable regulations. Failure to comply will result in sanctions, which can be criminal or administrative. In addition to providing a deterrent effect, sanctions can also provide lessons for violators, helping them

[1] Moh. Mahfud MD, 2011 "*Constitutional Law Debate: Post-Constitutional Amendment*". Jakarta: Rajawali Press. Page 52

DOI: https://doi.org/10.31933/1m23nk09

understand the dynamics of the law in a given environment. This is all very beneficial for improving public welfare.

Humans as*zoon politicon*According to Aristotle, social beings are constantly engaged in interactions with others. The need for social relationships is a form of self-actualization, which, according to Abraham Maslow, is the pinnacle of human needs. Humans express themselves to gain satisfaction and recognition from others. For thousands of years, these social interactions could only take place verbally or in writing, limited by distance and time.

The rapid development of technology has impacted various aspects of life, including economic, social, cultural, legal, and political aspects. These technological advances have transformed the way people communicate and even the way government services are provided to the public. Information and Communication Technology has become a new way for people to access information autonomously.[2] Technology has become a Human Right to Digital Access. The concept of Human Rights Protection (HAM) in the Digital Era reflects how modern information and communication technology affects individual rights;

1. Digital Privacy is the right of individuals to maintain the confidentiality of their personal data collected and processed in a digital environment.[3]
2. Transparency and Accountability, This concept emphasizes the importance of organizations, both government and private, to openly explain how personal data is used and provide accountability in the event of a privacy breach.[4];
3. Right to Be Forgotten, The right of individuals to have their personal information removed or deleted from search engines or websites if the information is no longer relevant or appropriate[5];
4. Non-discrimination in Algorithms, Preventing the use of algorithms that discriminate based on race, gender, or other attributes in decision-making that may affect individuals[6];
5. Freedom of Speech Online, Ensuring that individuals can speak, express opinions, and participate in digital spaces without censorship or unlawful restrictions.[7];
6. Online Anonymity Protection, Maintaining the right of individuals to participate anonymously in the digital world without revealing personal identity[8];
7. Digital Justice, Ensuring that access, benefits and harms of digital technologies are distributed fairly across society, including to vulnerable and disadvantaged groups.[9];
8. Cyber Security, Protecting individuals and organizations from cyber threats that can undermine an individual's right to have safe and secure information.[10];

This digital revolution has not only transformed the way we interact but has also influenced social and cultural values. With these technological advancements, we can share our personal lives on social media, conduct transactions online, and even hold meetings virtually.

The development of communication technology since entering the 21st century has

---

2 Raihana, et al., "The Influence of Technological Development on Legal Progress in Indonesia." Journal of Education and Counseling. Vol. 5. No. 2. 2023. Pp. 5628-5633

3 Westin, A. F. (1967). "Privacy and Freedom." Atheneum.hlm.69

4 Cavoukian, A., & Jonas, J. (2011). "Privacy by Design: The 7 Foundational Principles." Information and Privacy Commissioner of Ontario, Canada.hlm.75

5 Kosta, E. (2018). "The Right to Be Forgotten in the European Union: From Google Spain to the EU General Data Protection Regulation." International Data Privacy Law, 8(4), 267-282

6 Diakopoulos, N. (2016). "Algorithmic Accountability: A Primer." Data Society Research Institute.hlm.35

7 MacKinnon, R. (2012). "Consent of the Networked: The Worldwide Struggle for Internet Freedom." Basic Books

8 Nissenbaum, H. (1999). "The Meaning of Anonymity in an Information Age." The Information Society, 15(2), 141-144

9 Barocas, S., Hardt, M., & Narayanan, A. (2019). "Fairness and Machine Learning." Cambridge University Press

10 Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company

accelerated and undoubtedly influenced human interaction patterns. Social interactions, previously limited by distance and time, have become limitless. On the one hand, the digital revolution has increased connectivity, innovation, and convenience in various aspects of life.[11]. Human communication can be done orally or in writing *real time* Through digital media. This change in limitless communication channels makes it easier for people to establish social relationships. Besides these positive aspects, there are also negative impacts. In particular, the openness caused by technological advances can compromise the security of our personal data if not carefully considered. In today's digital or information age, science and technology are developing rapidly.[12]Social interactions through digital media not only create social relationships but also have the potential to cause conflict that can lead to losses, both material and immaterial.

Efforts to prevent and address conflicts arising from social interactions through digital media naturally utilize legal institutions. The need for laws to guarantee protection for digital media users is crucial, particularly regarding the security of their personal data. Laws must adapt to societal dynamics, including the transition of human interaction from the physical world to the virtual world.

Personal data protection in today's digital age has become essential. Munir explained that information and communication, as part of technology, also impact various aspects of life and change people's lifestyles and daily activities, including in the world of education, which utilizes digital media.[13]The rapid development of technology has had a profound impact on humanity. In general, the public is unaware of the impact of information misuse, leading to low awareness of personal data protection.[14]One of the impacts of this development is that humans must keep up with this rapid progress, which means they must not be left behind in this progress, so humans as a global society need to learn about it.

By studying these various digital developments, we can understand the various options and settings for utilizing this digitalization and maintaining the security of our personal data stored in digital media to prevent hacking or misuse by irresponsible individuals. Furthermore, the government is not turning a blind eye to these challenges. The Indonesian Internet Service Providers Association (APJII) announced that the number of internet users in Indonesia will reach 221,563,479 in 2024, out of a total population of 278,696,200 in 2023.[15]Digital media has become an inseparable part of modern society, due to its ability to provide a communication platform, increase insight and knowledge, and provide useful content.[16]Therefore, as a form of government concern for the public, who are both users and actors in digital development, various regulations and rules have been established to provide legal protection for all citizens in utilizing the currently rapidly developing digital advancements.

Law No. 27 of 2022 concerning Personal Data Protection was enacted due to numerous data breaches in Indonesia. One such breach involved the leak and sale of 91 million Tokopedia accounts. Criminals at Tokopedia sold data on the dark web, including user IDs, email

---

[11] Agbaji, D., Lund, B., & Mannuru, N. R. (2023). Perceptions of the Fourth Industrial Revolution and Artificial Intelligence Impact on Society. ArXiv Preprint ArXiv:2308.02030

[12] Khairul Anam, et al., “Effectiveness of Using Digital Media in the Teaching and Learning Process”. Drumang Asa: Journal of Primary Education. Vol. 2. No. 2. 2021. pp. 76-87

[13] Marjuni, A., & Harun, H. (2019). The Use of Online Multimedia in Learning. Idaarah: Journal of Educational Management, 3(2), 194–204

[14] Jeane Neltje Saly, et al., "Analysis of Personal Data Protection Related to Law No. 27 of 2022." Jurnal Serina Sosial Humaniora. Vol. 1, No. 3, October 2023: pp. 145-153

[15] APJII Number of Indonesian Internet Users Reaches 221 Million People.apjii.or.id.https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orangaccessed on August 22, 2024

[16] Adzan Zuhri, et al., "Utilization of Digital Media to Improve the Intellectual Capacity of the Young Generation at Nafidatunnajah Islamic Boarding School". Abdi Journal Publication. Vol. 1. No. 3. 2023. pp. 327-332

addresses, full names, birth dates, genders, mobile phone numbers, and hashed or encrypted passwords.[17]The latest case of a data leak is that the Ministry of Communication and Information Technology is suspected to be the victim of a data leak with a number of data ranging from NIK to bank accounts being hacked and sold on the dark web site "BreachForums"[18]Therefore, the author will write about the Civil Liability of Digital Platforms for Personal Data Leaks Following the Enactment of Law Number 27 of 2022 concerning Personal Data Protection.

RESEARCH METHODS

This legal research is a legal research. According to Peter Mahmud Marzuki, normative legal research is a process of discovering legal rules, legal principles, and legal doctrines to address the legal issues faced.[19]There are four approaches used. First, the Legal approach (*statue approach*) by examining various laws, regulations, and legal issues related to the research object, so that the consistency and suitability between one law and other laws that are still in effect can be seen. Second, the conceptual approach (*conceptual approach*) which is based on the views and doctrines that have developed in the science of law.

RESEARCH RESULTS AND DISCUSSION

Protection of Personal Data in Law Number 27 of 2022 concerning Protection of Personal Data in Indonesia;

Indonesia has ratified personal data protection regulations since 2022. In ratifying personal data protection regulations, it will be effective starting in 2024. Indonesia initiated personal data protection regulations because it is important for the government to monitor and protect the ownership of Indonesian people's data and data belonging to foreign parties in Indonesia so as to provide stability and foreign confidence to be able to make economic investments in Indonesia. The Indonesian Constitution has indirectly mandated the need for personal data protection regulations as regulated in Article 28F paragraph (1) and Article 28G paragraph (1) of the 1945 Constitution, as follows;

> **Article 28F paragraph (1)**
> *Everyone has the right to communicate and obtain information to develop their personality and social environment, and has the right to seek, obtain, possess, store, process and convey information using all available channels.*
>
> **Article 28G paragraph (1)**
> *Everyone has the right to protection of themselves, their family, their honor, their dignity and the property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a human right.*

The regulations governing personal data protection, as stipulated in Law Number 27 of 2022, consist of 16 chapters and 76 articles, covering a wide range of topics, from the definition of personal data, data controller obligations, data subject rights, and sanctions for violators. The following is the regulatory framework for personal data protection as stipulated in Law Number

[17] Adhi Wicaksono, "Complete Chronology of 91 Million Tokopedia Accounts Leaked and Sold". cnnindonesia.com.https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-24dan-dijualaccessed on 22 September 20

[18] Claimed 2021-2024 Domestic Domestic Data Sold for IDR 1.98 Billion on Illegal Forums."cnnindonesia.com.https://www.cnnindonesia.com/teknologi/20240702104538-192-1116574/data-diklaim-dari-pdn-2021-2024-dijual-rp198-m-di-forum-gelapaccessed on September 22, 2024

[19] Mahmud Marzuki, Legal Research (Prenada Media 2005).30

27 of 2022:[20]

1) Definition and Categories of Personal Data;
   According to Article 1 of the Personal Data Protection Law, personal data is data about an individual that is identified either directly or indirectly. The Law classifies personal data into two main categories. First, general data, which includes basic information such as full name, gender, religion, and marital status. Second, specific, sensitive data, such as health data, biometric data, genetics, criminal records, child data, and financial data. This distinction is important so that data management can be tailored to its level of confidentiality.
2) Data Protection Principles;
   The principles of the PDP Law form the basis for processing personal data. These principles include transparency, accountability, security, and consent from data subjects before data is processed. The authors also propose additional principles, namely:**non-discrimination**, which ensures that personal data may not be used for discriminatory purposes or to treat individuals unfairly based on race, religion, or political views. This will strengthen the protection of human rights and equality.
3) Data Subject Rights;
   Under Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), data subjects, individuals whose data is collected and processed, are granted various rights to protect their personal information. These rights aim to give individuals full control over their data, while ensuring that it is used transparently and responsibly by data controllers. Data subjects have the right to clearly understand how their personal data is collected, used, stored, and shared. They also have the right to grant or withdraw consent to data processing and to request the deletion of data that is no longer relevant or collected illegally. Furthermore, data subjects can object if their data is processed for purposes inconsistent with their initial consent and can even request the restriction of data processing to specific purposes.
4) Data Controller Obligations;
   Under Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), a data controller is the party that determines the purpose and has control over the processing of personal data. They can be from the public or private sector, such as government agencies, companies, organizations, or even individuals who manage a certain amount of data. Data controllers play a crucial role as they are at the forefront of maintaining the security and integrity of people's personal data. Therefore, the PDP Law stipulates a number of obligations that must be met to ensure data processing is carried out legally, transparently, and responsibly.
5) Sanctions under the Personal Data Protection Act
   To enforce compliance, the PDP Law establishes two types of sanctions. First, administrative sanctions in the form of fines that can reach 2% of a company's annual revenue. Second, criminal sanctions are applied for serious violations, such as the illegal sale of personal data. This distinction provides flexibility in law enforcement, where minor violations can be handled administratively, while serious violations are processed through criminal channels.

Considering the legal framework in Law Number 27 of 2022 concerning Personal Data Protection, it is the obligation of digital media organizers or platforms to comply with it. In operating a digital platform in Indonesia, every digital platform is required to register with the Ministry of Communication and Digital (Komdigi) as an administrative compliance measure. The requirement for every digital platform to register with Komdigi is mandated by

[20] Moody R. Syailendra, "Personal Data Protection and the Implementation of the Nomor 27 of 2022". Untar. Faculty of Law.https://fh.untar.ac.id/2025/09/11/perlindungan-data-pribadi-implementasi-uu-no-27-tahun-2022-dan-tantangan-penegakannya/accessed on December 8, 2025.

Government Regulation Number 71 of 2019 (PP Number 71 of 2019) concerning the Implementation of Electronic Systems and Transactions and Regulation of the Minister of Communication and Informatics Number 5 of 2020 concerning Private Electronic System Organizers (Perkominfo Number 5 of 2020). The obligation for every digital platform to register with Komdigi is also in line with the mandate of Law Number 27 of 2022 concerning Personal Data Protection regarding the "Obligations of data controllers" who should have a role in controlling and mastering all personal data belonging to Indonesian and foreign citizens residing in Indonesia.

Registering digital platforms under applicable regulations also aims to facilitate law enforcement in enforcing the law against platforms that harm or misuse the personal data of their citizens. It is known that digital platforms have become an integral part of modern society as a socio-technical ecosystem that facilitates interactions between users, providers, and third parties, with platforms such as Facebook, Instagram, YouTube, TikTok, and Tokopedia in Indonesia playing a crucial role in communication, commerce, and social interaction.[21]This is why it's crucial for every digital platform to register with Komdigi so the government can effectively monitor its citizens' interactions in the digital world.

Aspects of digital platforms encompass economic, social, political, and other activities, all of which play a crucial role in government protection. Law No. 27 of 2022 concerning the Protection of Personal Data is a way to assist the government in addressing the challenges of transparency in today's era, particularly the spread of illegal content. This highlights the need for a robust regulatory framework, as governance is crucial for balancing platform openness with user protection and maintaining social order.[22].

Personal data protection in Indonesia is a way to address legal uncertainty surrounding the protection of personal data belonging to Indonesian citizens. However, after Law Number 27 of 2022 concerning Personal Data Protection was passed into law and implemented in society, it still faces shortcomings, which pose obstacles to its implementation. One of the obstacles to the implementation of Law Number 27 of 2022 concerning Personal Data Protection is the lack of implementing regulations, the lack of a supervisory body, and the lack of a legal framework.*data protection officer* (DPO) as the party that monitors and enforces the law regarding personal data belonging to citizens in Indonesia. Insecurity and lack of oversight in the management of personal information have created the risk of data misuse, which can harm data owners.[23]The above obstacles to Law Number 27 of 2022 concerning personal data protection constitute imperfections in its implementation in society, resulting in uncertainty, thus hindering effective law enforcement as envisioned by the regulation.

Personal Data Surveillance in Indonesia

The increasing number of personal data breaches in Indonesia in the last few years has become a very serious issue, requiring an institution that can monitor crimes involving personal data in Indonesia.[24]. It is known that there has been an increase in cases in recent years related to personal data crimes in Indonesia. The government, in Law Number 27 of 2022 concerning Personal Data Protection, has regulated agencies that can protect its citizens so that data leaks can be detected quickly and responsively. The form of personal data oversight in Indonesia is

[21] Rabith Madah Khulaili Harsya, "A Legal Review of Digital Platform Responsibility for Illegal Content According to Indonesian Law". Sanskara Law and Human Rights Vol. 4, No. 01, August 2025, pp. 276-286

[22] Kirchner, S., & Schüßler, E. (2019). The organization of digital marketplaces: Unmasking the role of internet platforms in the sharing economy. Organization Outside Organization, 131–154.

[23] Danil Erlangga Mahameru, et al., "IMPLEMENTATION OF THE PERSONAL DATA PROTECTION LAW ON THE SECURITY OF IDENTITY INFORMATION IN INDONESIA". Journal of Legal Essence. Volume 5 No. 2 December 2023. Pp. 115-131

[24] Sayyidah Nafisah and Ayon Diniyanto, "Independence of Personal Data Protection Institutions in Indonesia". Manabia. Journal of Constitutional Law. Vol. 04, No. 01, Jul 2024: 1-20

regulated in Article 58 paragraphs (1) to (5) of Law Number 27 of 2022, namely:

Article 58 paragraph (1)
The government plays a role in implementing Personal Data Protection in accordance with the provisions of this Law.

Article 58 paragraph (2)
The implementation of Personal Data Protection as referred to in paragraph (1) is carried out by the institution

Article 58 paragraph (3)
The institutions referred to in paragraph (21) are determined by the President

Article 58 paragraph (4)
The institutions referred to in paragraph (21) are responsible to the President.

Article 58 paragraph (5)
Further provisions regarding the institutions as referred to in paragraph (2) are regulated by Presidential Regulation.

Under the aforementioned provisions, a supervisory agency to prevent and enforce the law against personal data crimes in Indonesia has not yet been established, as the government has not issued any derivative regulations or presidential regulations regarding the establishment of such an agency. Essentially, the establishment of a supervisory agency for the implementation of personal data protection is mandatory for the continued implementation of Law Number 27 of 2022 concerning personal data protection in Indonesia. The author reveals that enforcement of personal data protection in Indonesia, as regulated by Law Number 27 of 2022, has not been effective. This is due to the government's unpreparedness and inability to accommodate the implementation of law enforcement regarding personal data protection in Indonesia.

The existence of an independent body is key to ensuring independence in the monitoring, auditing, and prosecution processes. Essentially, a personal data protection oversight body in Indonesia is an effort to prevent and control cases of personal data leaks in Indonesia. In fact, this body is an effort to increase foreign investment confidence in Indonesia, as important data stored in Indonesia will feel secure and protected during business activities. The primary reason why an independent personal data protection oversight body in Indonesia has not yet been established is because "...[25]There are differences of opinion between the DPR and the government regarding the institutional design, especially whether it is under the ministry (Kominfo) or truly independent, as well as obstacles in the preparation of derivative regulations such as crucial Government Regulations (PP), resulting in a tug of war of interests and a time-consuming harmonization process despite the high urgency of overcoming data leaks.

The ongoing debate over the institutional design for oversight of personal data protection in Indonesia has fueled the rise in personal data crimes, resulting in continued data breaches. Data from the Institute for Policy Research and Advocacy (Elsam) in January 2024 also revealed that at least 668 million pieces of personal data were leaked across six major digital platforms. The leaked data included identity numbers, family card numbers, transaction

[25] Agus Tri Haryanto: "The PDP Institution Has Not Yet Been Formed, Minister of Communication and Digital Reveals the Reason" in fullhttps://inet.detik.com/law-and-policy/d-8142195/lembaga-pdp-masih-belum-dibentuk-menkomdigi-ungkap-alasannya. Accessed on December 8, 2025

histories, and biometric data.[26]The author analyzes that personal data leaks in Indonesia pose a serious threat, requiring the government to immediately establish a design for a personal data protection oversight agency without wasting time in debates until implementing the implementing regulations.

Despite the enactment of Law No. 27 of 2022, the level of personal data protection security in Indonesia remains a limited guarantee for data breach management. This is because the law lacks any implementing regulations to enforce personal data protection. Without the PDP (Personal Data Protection Agency) in place, personal data protection in Indonesia remains little more than a legal norm.[27]. The oversight agency for personal data enforcement in Indonesia has an important function, particularly in handling public reports of personal data leaks and providing guidelines for resolving disputes through legal channels, if necessary.

Previously, there was indeed pessimism regarding the formation of a Personal Data Protection Agency, or PDP for short. This is because, in the provisions of Article 58 paragraph (3) of Law Number 27 of 2022 concerning Personal Data Protection, the formation of a personal data protection supervisory agency will be regulated through a presidential regulation as well as its implementing regulations. Essentially, the PDP agency is key to enforcing compliance with PDP standards and obligations, from data controllers and processors. This means that without a strong PDP agency, it is difficult to implement the PDP Law effectively, including in guaranteeing the protection of data subjects' rights. Therefore, ideally, this agency is designed as an independent authority, both in terms of position, institution, duties and functions, and budgeting.[28]Therefore, the effectiveness of personal data oversight in Indonesia remains a written norm and has not yet been implemented due to the lack of an independent personal data protection oversight agency for prevention, enforcement, protection, and dispute resolution. The absence of a personal data oversight agency in Indonesia means that the level of security and protection of personal data remains uncertain and vulnerable to data leaks at any time. Therefore, law enforcement in personal data oversight in Indonesia remains the same as before the enactment of Law Number 27 of 2022 concerning Personal Data Protection.

Civil Liability of Digital Platforms for Data Leaks According to Law Number 27 of 2022 Concerning Personal Data Protection

1. The Concept of Civil Liability

Civil liability is essentially a legal obligation arising from an act that harms another party. This concept requires the perpetrator to compensate for the losses incurred, whether intentional or negligent. The goal is to restore the injured party to the condition they were in before the loss occurred, ensuring justice for you as the victim.

In the context of digital platforms, civil liability arises when they fail to protect personal data. This failure, which can include negligence in security systems, is considered an act that causes harm. This harm can include not only material harm, such as loss of money,

[26] Iqbal Basyari: "Personal Data Leaks Continue to Threaten, Oversight Body Still Unformed."https://www.kompas.id/artikel/kebocoran-data-pribadi-terus-mengancam-lembaga-pengawas-tak-kunjung-dibentuk?status=sukses_login&utm_source=kompasid&utm_medium=login_paywall&utm_campaign=login&utm_content=https://www.kompas.id/artikel/kebocoran-data-pribadi-terus-mengancam-lembaga-pengawas-tak-kunjung-dibentukaccessed on December 8, 2025

[27] Salsa Nabila Hardafi, "The Absence of PDP Institutions: Legal Loopholes in Personal Data Protection".hukumonline.com.https://www.hukumonline.com/berita/a/ketiadaan-lembaga-pdp--celah-hukum-dalam-pelindungan-data-pribadi-lt686d4f5817d73/?page=4accessed on December 8, 2025

[28] Institute for Policy Research and Advocacy (ELSAM), "Personal Data Protection Institution, Key to Enforcing Compliance with the PDP Law". elsam.or.id.https://www.elsam.or.id/siaran-pers/lembaga-pelindungan-data-pribadi--kunci-penegakan-kepatuhan-uu-pdpaccessed on December 8, 2025

but also immaterial harm, such as damage to your reputation or psychological distress.

Law Number 27 of 2022 concerning Personal Data Protection strengthens the legal basis for pursuing this civil liability. The law establishes specific obligations for digital platforms to safeguard data. When a breach occurs due to a breach of these obligations, the platform can no longer evade responsibility. This regulation provides a stronger basis for you to pursue compensation in civil court.

2. Definition and Elements of Civil Liability

Civil liability, by definition, is a legal obligation to compensate for losses caused by an unlawful act. In the case of a data breach, if a digital platform is proven negligent and causes you harm, they have an obligation to reimburse you for those losses. This concept provides the legal basis for your claim for justice.

To prove civil liability, several elements must be met. First, there must be an unlawful act by the platform, such as violating security obligations under the PDP Law. Second, there must be error or negligence on the part of the platform. Third, you must be able to prove that a loss has occurred, whether material, such as the loss of money, or immaterial.

The final, equally important element is a causal link between the platform's negligence and the loss you experienced. You must be able to demonstrate that the loss was a direct result of the platform's failure to secure your data. If all of these elements are met, the platform will be liable.Digital is obliged to provide compensation according to the court's decision.

Civil Liability of Digital Platforms Following Law Number 27 of 2022 Concerning Personal Data Protection

Following the enactment of the PDP Law, the civil liability of digital platforms is no longer unclear. This law clearly places the burden of responsibility on them as data controllers. If a breach occurs due to a security system failure, they can no longer avoid legal responsibility to compensate you for the losses you have suffered as a data subject.

This civil liability arises from the failure of digital platforms to comply with various obligations mandated by the PDP Law. These obligations include implementing reliable security systems and lawful data processing. Failure to meet these data protection standards is considered a direct misconduct that causes harm to you, thus opening the way for civil claims.

The PDP Law also strengthens your position by placing the burden of proof on the digital platform itself. In the event of a breach, they must be able to demonstrate that they implemented all required protective measures. Failure to demonstrate compliance automatically strengthens your claim for compensation for the losses you suffered as a result of the incident.

1. Forms of Civil Liability Due to Data Leaks

The most important form of civil liability is material damages. This is compensation for quantifiable financial losses directly resulting from a data breach. For example, if your data is misused to drain your bank account, the costs you incur for obtaining new documents, or other financial losses that can be proven to be a direct result of the incident.

In addition to financial losses, the PDP Law also recognizes immaterial compensation. This form of liability is intended to redress non-material losses you've experienced, such as psychological distress, fear, or defamation. These types of losses are often more difficult to quantify, but the law recognizes the mental and reputational impacts of having your personal data exposed.

Judges can also order digital platforms to take certain actions as part of their civil liability. These orders could include requiring them to publicly disclose data breaches or implement security system improvements. The goal is not only to provide compensation but

also to ensure the platform corrects its negligence and prevents similar incidents from happening again.

2. Mechanism for Claiming Compensation by Data Subjects

If a data subject becomes a victim of a data breach, the first legal step is to file a lawsuit.civil suit to district courtLaw Number 27 of 2022 concerning Personal Data Protection provides a strong legal basis for you to sue for damages. In this lawsuit, you will need to outline how the digital platform was negligent and failed to protect your data, resulting in the harm you suffered as a data subject.

In court, you, as the plaintiff, have the burden of proving several things. You must demonstrate unlawful conduct by the platform, actual harm, and a causal link between the platform's negligence and that harm. Evidence can include transaction evidence, correspondence, or security audit reports demonstrating negligence on the part of the digital platform.

Apart from individual lawsuits, if the data leak affects many people, you can take the following mechanisms: class action lawsuit This option allows victims to unite and collectively demand their rights. Law Number 27 of 2022 concerning Personal Data Protection also mandates the establishment of an institution to assist in dispute resolution, which could later serve as an alternative out-of-court settlement.

3. Law Enforcement Challenges to Civil Liability

One of the main challenges in enforcing civil liability is proof. Data subjects, as victims, often have difficulty proving technical negligence.*platform*Furthermore, directly linking the losses experienced by data subjects to data breach incidents presents a challenge, particularly for immaterial losses, which are subjective and difficult to quantify with precise figures.

The effectiveness of the supervisory agency mandated by Law Number 27 of 2022 concerning Personal Data Protection will be a crucial factor. Another challenge is the readiness of law enforcement officials, including judges, to handle technically complex personal data disputes. Expensive litigation costs and lengthy court processes can also be significant barriers to pursuing individual compensation.

Nevertheless, the prospects for enforcement remain bright. The presence of the PDP Law itself has provided a much stronger legal basis for you. The potential for class action lawsuits (*class action*) also paves the way for victims to unite and collectively fight for their rights. Increased public awareness will continue to drive better law enforcement in the future.

CONCLUSION

Indonesia has enacted personal data protection regulations since 2022. The ratification of the personal data protection regulations is expected to be effective starting in 2024. When Law Number 27 of 2022 concerning personal data protection was enacted into law and implemented in society, it still had shortcomings, which became obstacles to its implementation in society. One obstacle in the implementation of Law Number 27 of 2022 concerning personal data protection was the lack of derivative regulations. The lack of derivative regulations in the implementation of Law Number 27 of 2022 was due to ongoing debate within the government, such as the institutional model for overseeing personal data protection in Indonesia. In fact, this debate within the government also resulted in the lack of the formation of a national data protection agency. *Data Protection Officer* (DPO), or the officer who oversees any organization or company that manages or collects personal data belonging to other legal entities. The aforementioned obstacles indicate that the government

has not provided certainty regarding the implementation of Law Number 27 of 2022 concerning personal data protection, and the regulations are merely paper norms. Therefore, digital media users in Indonesia remain at significant risk of personal data leaks when conducting transactions within these digital media platforms.

In the context of digital platforms, civil liability arises when they fail to protect personal data. This failure, which can include negligence in security systems, is considered an act that causes harm. Following the enactment of the PDP Law, the civil liability of digital platforms is no longer unclear. This law clearly places the burden of responsibility on them as data controllers. If a leak occurs due to a security system failure, they can no longer avoid legal responsibility to compensate for the losses suffered by you as the data subject. The most important form of civil liability is material damages. This is compensation for directly quantifiable financial losses resulting from the data breach. One of the main challenges in enforcing civil liability is proving the cause. Data subjects, as victims, often struggle to prove specific technical negligence on the part of the platform. Furthermore, directly linking the losses suffered by data subjects to the data breach incident presents a challenge, especially for immaterial losses, which are subjective and difficult to quantify.

REFERENCE

Barocas, S., Hardt, M., & Narayanan, A. (2019). "Fairness and Machine Learning." Cambridge University Press

Cavoukian, A., & Jonas, J. (2011). "Privacy by Design: The 7 Foundational Principles." Information and Privacy Commissioner of Ontario, Canada

Diakopoulos, N. (2016). "Algorithmic Accountability: A Primer." Data Society Research Institute

MacKinnon, R. (2012). "Consent of the Networked: The Worldwide Struggle for Internet Freedom." Basic Books

Moh.Mahfud MD, 2011 "*Constitutional Law Debate: Post-Constitutional Amendment*". Jakarta: Rajawali Press

Schneier, B. (2015). "Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World." W. W. Norton & Company

Shinta Dewi Rosadi, Cyber Law: Aspects of Data Privacy According to International, Regional, and National Law, First Edition, PT Refika Aditama, Bandung, 2015

Adzan Zuhri, et al., "Utilization of Digital Media to Improve the Intellectual Capacity of the Young Generation at Nafidatunnajah Islamic Boarding School". Abdi Jurnal Publikasi. Vol. 1. No. 3. 2023. pp. 327-332

Amar Ahmad, "The Development of Communication and Information Technology: The Roots of the Revolution and Its Various Standards." Tabligh Dakwah Journal, Vol. 13, No. 1, June 2012: 137–149

Danel Aditia Situngkir, "The Bound of States in International Agreements." Legal Reflections. Volume 2 Number 2, April 2018, Pages 167-180

Danil Erlangga Mahameru, et al., "IMPLEMENTATION OF THE PERSONAL DATA PROTECTION LAW ON THE SECURITY OF IDENTITY INFORMATION IN INDONESIA". Journal of Legal Essence. Volume 5 No. 2, December 2023. Pp. 115-131.

Elfian Fauzi and Nabila Alif Radika Shandy, "The Right to Privacy and the Legal Politics of Law Number 27 of 2022 Concerning Personal Data Protection." LEX-Renaissance NO. 3 VOL. 7 JULY 2022. pp. 445-461

Erna Priliasari, "The Importance of Personal Data Protection in Online Loan Transactions." National Law Magazine. Vol. 49. No. 2. 2019. pp. 1-27

Evi Rosdiyanti and Abustam, "International Law as a Source of Law in National Law." JIHAD: Journal of Law and Administration. Vol. 2 No. 2 September 2020. pp. 21-34

Farid Ahmadi Sunyoto and Anidya Ardiansari, "The Influence of Online Trading on the Behavior of Semarang City Residents." Riptek Vol. I2, No. 2, 2018, pp. 107-118

Indriana Firdaus, "Legal Protection Efforts for Privacy Rights Against Personal Data from Hacking Crimes." RECHTEN JOURNAL: LEGAL AND HUMAN RIGHTS RESEARCH. Vol. 4. No. 2. 2022. pp. 22-31

I Made Sugita, "Legal Protection of the Right to Population Administration Services at the Population and Civil Registration Office of Karangasem Regency." Jayapangus Press Metta: Journal of Multidisciplinary Science. Volume 2 Number 3 (2022). pp. 119-132

The 1945 Constitution of the Republic of Indonesia

Law Number 1 of 1946

Law Number 36 of 1999 concerning Telecommunications

Law Number 39 of 1999 concerning Human Rights

Law Number 14 of 2008 concerning Public Information Disclosure

Law Number 36 of 2009 concerning Health

Law Number 24 of 2013 concerning Population Administration

Law Number 30 of 2014 concerning Government Administration

Law Number 27 of 2022 concerning Personal Data Protection

Minister of Communication Regulation Number 5 of 2020 concerning Personal Data Protection