Journal Equity of Law and Governance
Volume 7, Nomor 1, Page: 10-21
https://ejournal.warmadewa.ac.id/index.php/elg/index

Online ISSN 2776-5121
Print ISSN 2775-9512

https://doi.org/10.22225/elg.7.1.11938.10-21

The urgency of protecting sensitive data is reflected in Article 4(2) of Law No. 27/2022 on Personal Data Protection

Andi Darti[1], and Marnija[1]

1. Universitas Borobudur, Indonesia

Coressponding author;
Andi Darti, Universitas Borobudur, Indonesia
Email: andidarti@gmail.com

Abstract. The protection of personal data is a top priority in the digital era, especially with the increasing threats to individual privacy and security of sensitive information such as health, biometric, and genetic data. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is present as a legal framework that emphasizes the principles of transparency, security, and accountability to prevent data misuse. However, the implementation of the PDP Law in Indonesia faces significant challenges, such as technological limitations, low awareness among Electronic System Operators (PSEs), and weak law enforcement mechanisms. This study aims to analyze the effectiveness of Article 4(2) of the PDP Law in protecting sensitive data and explore strategic steps to overcome implementation constraints. The research methods used are normative research with juridical and conceptual approaches, as well as qualitative analysis. The juridical approach analyzes legal texts, while the conceptual approach explores the best practices of international regulations such as the EU GDPR. The data was analyzed descriptive-analytically to identify obstacles and solutions. The results of the study show that strengthening supervision, the adoption of advanced technologies such as AI and blockchain, and public education are urgently needed. This research recommends synergy between the government, PSE, and the community to create a safe and reliable digital ecosystem, while supporting digital transformation and sustainable economic growth.

Keywords: enforcement; regulation; security.

INTRODUCTION

Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is an important milestone in the regulation of data protection laws in Indonesia. Article 4(2) of the PDP Law highlights the urgency of protecting sensitive data as an integral part of the privacy rights of individuals. Sensitive data, which includes information such as health data, biometrics, genetic data, and personal beliefs, has great potential for misuse if not adequately protected (Tari Oktaviani & Nailufar, 2023). With the increase in digitalization in various sectors, the risk of sensitive data breaches is getting higher, so regulations that regulate the principles of transparency, accountability, and security in data processing are crucial (Law No. 27 of 2022). These principles aim to prevent data-based discrimination and guarantee individuals' right to privacy in the digital age.

Although the ratification of the PDP Law is a significant step, its implementation in the field still faces major challenges. One of the main obstacles is the low-security standards implemented by Electronic System Operators (PSEs), which often leads to the leakage of sensitive data such as health and biometric data. An example of a case that is often in the spotlight is the incident of health data leakage in the public service sector which results in losses for individuals and has the potential to reduce

public trust in the data protection system (Directorate General of Informatics Applications, Ministry of Communication and Informatics, 2020). In addition, the low awareness of the public about their rights to protect personal data is also a factor that worsens the situation. Many individuals are unaware that they have the right to know, access, and control the use of their data in accordance with the PDP Law.

Shopping online through e-commerce platforms does provide convenience, but it also has the potential to pose risks for users, such as misuse of personal data (Um, 2018). The weak personal data protection system (PDP) causes cases of e-commerce user data leaks to continue to occur. In the 2019–2020 period, tens of millions of e-commerce platform user data were targeted for theft, such as 91 million Tokopedia user data, 1.2 million from Bhinneka.com, and 13 million from Bukalapak (Pusparisa, 2020). In 2020 alone, the National Consumer Protection Agency (BPKN) received 1,276 reports related to the e-commerce sector, the majority of which were related to phishing and account abuse through one time password (OTP) (CNN Indonesia, 2020). The rampant misuse of this data shows that the management of personal data in Indonesia still has serious security gaps. The lack of regulations that specifically regulate PDP has also exacerbated the situation (Aswandi et al., 2020). This is very different from countries such as Hong Kong, South Korea, the Philippines, and the European Union, which have had personal data protection regulations for a long time (Doly, 2021; Sangojoyo et al., 2022). Data leak incidents almost always occur every year. For example, in 2023, the State Cyber and Cryptography Agency (BSSN) reported 149 alleged data leaks, consisting of 50 incidents and 99 proactive notifications from the dark web, which impacted 129 related parties (BSSN, 2023).

To address these challenges, the government has a strategic role to play in ensuring PSEs comply with the set standards for protecting sensitive data. Technical measures such as the use of data encryption, multi-factor authentication, as well as risk-based monitoring systems, are urgently needed to prevent unauthorized access and misuse of data (Smart Legal, 2021). However, surveys show that only a small percentage of PSEs have adequately implemented these security measures, so incidents of data breaches are still frequent. In addition, regulatory oversight of PSEs needs to be strengthened through periodic audits, security certification, and the imposition of strict sanctions for violators. Strong sanctions not only serve as a deterrent but also to restore public trust in Indonesia's data protection system (Sustain Indonesia, 2024).

On the other hand, comparative studies with international legal frameworks such as the EU's General Data Protection Regulation (GDPR) show that strong regulation requires good infrastructure support, cross-sector collaboration, and broad public education. The GDPR, for example, mandates the appointment of a Data Protection Officer (DPO) in organizations that process sensitive data as an additional accountability measure (European Union, 2018). The same thing can be adapted in the Indonesian context to strengthen the implementation of the PDP Law. Therefore, the Indonesian government needs to take strategic steps to ensure that existing regulations are not only symbolic but can also be implemented effectively to protect sensitive public data.

In the Introduction, the Author must state the purpose of the work at the end of the introduction section. Prior to the objectives, the author should provide an adequate background, and a very brief literature survey to note the existing solutions/methods, to show which are the best of the previous research, to show the main limitations of the previous research, to show what you want to achieve (to solve the limitations), and to show the scientific benefits or novelty of the paper. Avoid detailed literature surveys or summary results.

METHOD

This study uses normative legal research methods with a juridical approach and qualitative analysis. The juridical normative approach is used because this research focuses on the analysis of legal texts, especially Article 4(2) of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), as well as its relevance in protecting sensitive data. This method includes the study of laws and regulations, legal

documents, and scientific literature to identify, interpret, and evaluate the principles contained in related regulations. Juridical normative research also allows researchers to analyze the strengths and weaknesses in existing regulations and provide recommendations for the improvement of the legal system (Marzuki, 2017). In addition, this study uses a conceptual approach to understand the concept of sensitive data protection holistically, including comparisons with similar regulations at the international level, such as the General Data Protection Regulation (GDPR) in the European Union. The conceptual approach aims to explore a deep understanding of the definition, scope, and urgency of protecting sensitive data that has become a global issue (Salim & Nurbani, 2013). This approach helps identify best practices that can be adapted to the Indonesian context.

The qualitative analysis in this study was carried out to explore the patterns, relationships, and implications of the application of Article 4(2) of the PDP Law in the field. The data was analyzed in a descriptive-analytical manner with an emphasis on evaluating the implementation of regulations, the obstacles faced, and strategic measures to overcome sensitive data breaches. This analysis also involves the interpretation of data leak reports, relevant case studies, and the results of interviews with stakeholders, including regulators and electronic system operators (Sugiyono, 2016). This research is also equipped with a comparative approach to analyze the differences and similarities between the PDP Law and similar regulations in other countries. Thus, this study not only examines the normative aspects but also identifies gaps in the implementation of data protection regulations in Indonesia. This is expected to provide practical recommendations to the government and related parties to improve the security of sensitive data in the digital era. By using this multi-method approach, this study is able to present a comprehensive picture of the urgency of protecting sensitive data in the context of the PDP Law. This approach also allows for the identification of the strategic measures necessary to ensure the successful implementation of the regulation in protecting the privacy of individuals in Indonesia

RESULTS AND DISCUSSION

The protection of personal data is closely related to the right to privacy, which is an inseparable part of human rights. From the perspective of Komnas HAM (2021), every individual has the right to control their personal data, including determining who can access, process, or use the data. This right to privacy includes the assurance that personal data will not be misused by any party for purposes that are detrimental to the individual. When personal data, especially those of a sensitive nature, is not properly protected, the consequences can be serious privacy violations, intimidation, discrimination, or even exploitation that undermines human dignity.

Komnas HAM emphasized that the leak of personal data is a form of severe violation of the right to privacy. When sensitive information, such as health, biometric, or sexual orientation data, falls into the wrong hands, individuals not only lose control of their information but also become vulnerable to various forms of threats. This kind of violation can create insecurity, psychological pressure, and the risk of exploitation, such as economic manipulation or extortion. In this context, the state has an obligation to protect the basic rights of individuals by ensuring that personal data protection regulations are implemented effectively.

In addition, Komnas HAM highlighted the impact of social discrimination and stigmatization that can arise due to the misuse of sensitive data. Personal data related to health status, religious beliefs, or sexual orientation are often used to create stereotypes or stigmas in society. This not only impacts individuals' social lives but also hinders their opportunities to gain equal access to employment, education, or public services. For example, a health data leak can result in a person losing their job or being rejected by an insurance company, which is a real form of discrimination. Social stigma can also affect an individual's mental well-being, create social isolation, and exacerbate inequality.

Komnas HAM (2021) emphasizes the importance of a human rights-based approach in protecting personal data. This includes the principles of transparency in data management, adequate security guarantees, and accountability of the parties processing data. In addition, the state is also expected to provide an effective complaint mechanism for individuals who experience privacy violations. Legal protection must be accompanied by strict sanctions against violators to provide a deterrent effect while ensuring justice for victims.

In the Indonesian context, the protection of personal data regulated in Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) reflects the state's commitment to protecting citizens' right to privacy. However, Komnas HAM noted that the successful implementation of this regulation is highly dependent on consistent supervision, public education, and strengthening technological infrastructure. Without these measures, personal data protection will only become a legal norm that is difficult to implement in the field.

According to Privy.id (2021), the protection of personal data is becoming increasingly important in the digital era, where sensitive individual information is more easily accessed and misused without permission. Personal data, especially those concerning sensitive aspects such as sexual orientation, religious beliefs, or other personal status, requires strict safeguards to prevent serious negative impacts. When this sensitive data is disclosed without consent, individuals not only lose control over their privacy but are also vulnerable to various forms of harm. Misuse of this information can cause reputational damage, emotional trauma, and social exclusion which can have a negative impact on a person's personal and professional life.

For example, information about sexual orientation that is revealed to the public without consent can put individuals in a dangerous position, especially in an intolerant environment. This can trigger social stigma, physical threats, and even violence, which violate human rights and destroy individual dignity. In the context of religion, sensitive data about a person's beliefs also has the potential to be a tool for discrimination or attack, especially in a diverse and sometimes vulnerable society to religious conflicts. Misuse of this data can exacerbate social tensions, create prejudice, or hinder individuals' access to basic rights such as employment, education, and healthcare.

Privy.id (2021) emphasizes that the protection of personal data is not only about digital security but also about safeguarding human rights, protecting dignity, and ensuring social justice. Personal data must be managed with strict principles of transparency, security, and accountability. Every party involved in data management, including governments and electronic system operators, has a responsibility to ensure that individual data is not misused or accessed by unauthorized parties. In addition, strong legal and technological mechanisms are needed to provide maximum protection for personal data.

The importance of personal data protection is also related to the increasing threat of cybercrime, where sensitive data is often the main target. Attacks on this data not only have the potential to cause financial losses but can also be used for psychological manipulation, extortion, or broader privacy violations. Privy.id noted that measures such as data encryption, double authentication, and educating the public on the importance of protecting their data are key to creating a secure digital environment.

Overall, Privy.id (2021) concluded that the protection of personal data is not only an individual responsibility but also a collective responsibility involving the active role of the government, technology companies, and society. Adequate protection will ensure that individuals can live their lives without fear that their personal information will be used to their detriment.

Sensitive data breaches, particularly those related to scientific research or government policies, have a significant impact on a country's political and economic stability. According to the Ministry of Communication and Information Technology (Kominfo, n.d.), data leaks involving strategic information can disrupt the decision-making process at the national level. In the context of scientific research, for example, data that is not properly protected can be manipulated or used without permission for the benefit of certain parties. This not only harms researchers but also lowers the credibility of research results, ultimately influencing evidence-based policies designed in the public interest.

Within the scope of government policy, data breaches can lead to the disclosure of strategic information that should be confidential. For example, leaked data on economic development plans, fiscal policies, or national security strategies can be used by outsiders to weaken a country's position in international negotiations or create instability at home. Misused information can also trigger public distrust of the government, especially if this data breach has a direct impact on the rights and privacy of individuals. In some cases, data leaks have been used to manipulate public opinion through the dissemination of disinformation, which can disrupt democratic processes and create political uncertainty.

Furthermore, sensitive data breaches in economic sectors can destabilize markets. Leaked information about monetary or fiscal policy can be leveraged for adverse speculation, both in the stock market and the banking sector. Data leaks also have the potential to affect investor confidence, especially if it is considered that the government or related institutions are incapable of protecting strategic data. This can have an impact on investment flows and slow down economic growth.

Kominfo (n.d.) emphasized that to prevent this impact, a comprehensive approach is needed to managing sensitive data. Steps that can be taken include strengthening data protection regulations, implementing security technologies such as encryption, and stricter supervision of institutions that manage strategic data. Additionally, increasing awareness among policymakers about the importance of data protection is essential to ensure that sensitive data is managed to the highest security standards. By ensuring adequate protection, the government not only maintains public trust but also ensures sustainable political and economic stability.

Personal data protection plays an important role in building and maintaining public trust in the government and institutions responsible for the management of personal information. According to the Ombudsman (2021), compromising sensitive data, either through leaks or misuse, can undermine public trust in the ability of governments or corporate bodies to keep their information secure. When individuals feel that their personal data is not being managed properly, it not only reduces a sense of security but also reduces trust in digital services, which is an important pillar in today's digital transformation.

The impact of this loss of trust can be felt in various sectors. In public services, for example, the leakage of personal data involving health, biometric, or financial information can discourage people from using government digital services. In fact, the service is designed to improve efficiency and accessibility. This mistrust can also affect public participation in government programs that require data collection, such as social assistance programs or population censuses. As a result, the success of these programs can be hampered because the data collected is incomplete or inaccurate.

In the private sector, a company's inability to protect customer data can lead to significant reputational losses. Consumers who lose confidence in data security in a company tend to switch to competitor services that are considered more reliable. In the long run, companies that fail to protect personal data may experience a decline in market share and difficulty attracting investors, especially in an era where data protection is one of the main indicators of good corporate governance.

To prevent wider losses, the Ombudsman (2021) recommends that governments and corporate bodies adopt a more proactive approach to protecting personal data. This includes the implementation of advanced security technologies, such as data encryption and double authentication, as well as regular updates of security systems to address evolving cyber threats. In addition, there needs to be a transparency policy that ensures that people are clearly informed about how their data is managed and protected. This transparency is important to build public trust, especially when there is an incident of data breach so that the mitigation measures taken can be understood by the public.

Strict law enforcement is also needed to ensure that breaches of personal data protection are taken seriously. Strict sanctions for violators not only provide a deterrent effect but also show the government's commitment to protecting people's right to privacy. In addition, educating the public about the importance of protecting personal data and how to protect their information in the digital world is a strategic step to increase collective awareness.

Overall, the protection of personal data is not only a technical issue but also relates to broader social and political responsibilities. By managing personal data securely and transparently, governments and companies can create a digital environment that is trusted by society, support inclusive digital transformation, and ensure the sustainability of digital systems in the future.

Personal data protection has become an increasingly important global issue amid the rapid development of digital technology. Violations or misuse of personal data can have severe consequences, both for individuals and the wider community. In response to these challenges, various countries have developed legal frameworks to ensure better data protection. The European Union's General Data Protection Regulation (GDPR) and the Personal Data Protection Law (PDP) in Indonesia are prime

examples of this effort. Both regulations aim to provide legal guarantees for individuals of their privacy rights, ensuring that personal data is managed with the principles of transparency, security, and accountability (PinterPandai, n.d.).

The GDPR, which came into effect in May 2018, has become a global standard in the protection of personal data. These regulations provide individuals with strong rights to control their data, including the right to access, correct, and delete personal data. The GDPR also establishes an obligation for data controllers to provide maximum protection for the data they manage, with significant threat of sanctions in the event of a breach. One of the advantages of the GDPR is its proactive approach to preventing data breaches, such as requiring notification of breaches within 72 hours to authorities and affected individuals. This policy not only provides legal protection but also fosters public trust in the digital system (European Union, 2018).

In Indonesia, the PDP Law passed in 2022 provides a legal framework similar to the GDPR, although it still needs to be strengthened in law enforcement and technical implementation. The PDP Law affirms the right of individuals to control their personal data and requires electronic system operators to protect data with adequate security technology. In addition, the PDP Law also regulates the provision of sanctions to violators, although the level is lighter compared to the GDPR. This regulation reflects Indonesia's commitment to protecting individual privacy in the digital era, which is crucial in building public trust in digital services and data governance (Indonesia.go.id, 2022).

This international and local framework emphasizes the importance of collaboration between governments, the private sector, and the public in ensuring the protection of personal data. At the global level, the GDPR is the main reference for other countries in designing their data protection regulations, including Indonesia. Meanwhile, at the local level, the PDP Law provides a strong legal basis to protect personal data while encouraging the growth of a safe and trusted digital ecosystem.

However, challenges remain. In Indonesia, the implementation of the PDP Law faces obstacles such as a lack of public awareness, limited technological infrastructure, and weak supervision. Therefore, greater efforts are needed to improve public education, develop security technology, and strengthen law enforcement mechanisms. With these measures, personal data protection can be a key pillar in ensuring the security and sustainability of digital systems, both at the national and international levels.

Personal data protection has become a major issue at the global level, especially with the increasing threat of data breaches in the digital era. The European Union's General Data Protection Regulation (GDPR), which came into effect in May 2018, has become one of the most comprehensive regulations governing the management and protection of personal data. The GDPR establishes core principles such as transparency, accountability, and security in the management of personal data, and gives individuals a strong right to control their data. This regulation gives supervisory authorities the legal power to impose significant sanctions on violators, including fines of up to 4% of the company's global annual revenue or up to €20 million, depending on which is greater (Simbolon & Juwono, 2022).

The GDPR approach emphasizes not only passive data protection but also active prevention of data breaches. One of the important features of the GDPR is the obligation for data controllers to report data breaches to the relevant authorities within 72 hours of an incident being detected. This reporting also includes notifying affected individuals if the violation poses a high risk to their rights and freedoms. This provision is designed to ensure that data breaches are not only responded to quickly but also transparently, ultimately strengthening public trust in digital systems.

The GDPR also provides individuals with clear rights, such as the right to access their personal data, the right to rectify inaccurate data, the right to delete data (the right to be forgotten), and the right to restrict the processing of their data. These rights give individuals greater control over their data, which is at the core of privacy protection. In the context of companies, the GDPR requires data controllers to ensure that data is only collected and used in accordance with the explicit consent of the individual, and only for clearly defined purposes.

Strong law enforcement under the GDPR shows that the protection of personal data is not only a technical responsibility but also a serious legal obligation. With the threat of significant fines, the GDPR provides a strong incentive for companies to comply with regulations and adopt high-security standards.

This approach not only protects individuals from the negative impact of data breaches but also encourages companies to manage data more responsibly.

In a global context, the GDPR has become a model for many countries, including Indonesia, which has just enacted the Personal Data Protection Law (PDP Law) in 2022. Although the PDP Law has a similar structure, such as individuals' rights to their data and data breach reporting obligations, the level of sanctions in Indonesia is still lighter compared to the GDPR. However, the application of GDPR principles in the PDP Law reflects Indonesia's commitment to improving data governance in the digital era.

By establishing a robust framework, the GDPR has proven that strict regulation can improve data security, protect individual privacy rights, and build public trust in digital systems. This approach is an important example for other countries facing data protection challenges in the ever-evolving technological era.

Personal data protection in Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) affirms Indonesia's commitment to better data governance in the digital era. One of the important elements regulated in the PDP Law is the rights of data subjects, where individuals have full control over their personal data. This right includes access, modification, and deletion of personal data at the request of the data subject. This data subject right ensures that individuals can manage their information independently and provides transparency in data management by third parties (Indonesia.go.id, 2021).

In addition, the PDP Law requires data management entities to provide data breach notification to relevant parties within 72 hours after an incident is detected. These provisions are designed to minimize further risks that may arise as a result of data breaches and provide an opportunity for data subjects to take mitigation measures. This mechanism reflects the importance of transparency and accountability in the management of personal data, especially in the midst of the increasing threat of data breaches in the digital era.

The processing of personal data must also be based on the explicit consent of the data subject. This consent must be given explicitly and in an easy-to-understand form, ensuring that the data subject understands how their information will be used. In addition, the PDP Law limits data storage to only the necessary period of time in accordance with the purpose of collection. This provision aims to prevent the accumulation of irrelevant data and reduce the risk of data misuse.

However, although the PDP Law has a similar framework to the European Union's General Data Protection Regulation (GDPR), there are significant differences in the level of enforcement. Under the GDPR, regulatory violations can be subject to fines of up to 4% of a company's global annual revenue or up to €20 million, depending on which is greater. On the contrary, the sanctions in the PDP Law tend to be lighter, which can reduce the deterrent effect of violations. This difference shows the need to strengthen law enforcement in Indonesia to ensure stricter compliance with data protection regulations.

As a step to improve the implementation of the PDP Law, it is important for the government to strengthen the supervision and law enforcement mechanism. This includes periodic audits of data management entities, provision of technological infrastructure that supports data security, and education to the public on the importance of personal data protection. By adopting strong principles such as the GDPR, Indonesia can strengthen the protection of individual privacy rights while building public trust in data governance in the digital era.

The California Consumer Privacy Act (CCPA), which went into effect in January 2020, is one of the significant personal data protection regulations in the United States. The CCPA gives consumers the right to know what information is collected by the company, as well as to request the deletion of that data. The regulation also allows consumers to file personal lawsuits against companies that fail to protect their data or engage in data breaches. The CCPA's primary focus is to provide consumers with full control over their personal data, ensuring that any data collection and processing is done with transparency and accountability (California Department of Justice, 2020).

Despite its similarities to the European Union's General Data Protection Regulation (GDPR) and the Personal Data Protection Law (PDP Law) in Indonesia, the CCPA has a more focused approach to consumer rights without enforcement as strong as the GDPR. Under the CCPA, companies that violate

regulations can be subject to fines of up to $7,500 per violation, which is lower compared to sanctions under the GDPR that account for 4% of global annual revenue or up to €20 million. These lighter penalties reflect a more permissive approach to law enforcement under the CCPA, while still providing a legal mechanism that allows individuals to sue privately in data breach cases (California Consumer Privacy Act, 2020).

Like the GDPR and the PDP Law, the CCPA focuses on strengthening consumers' control over their personal data. These regulations require companies to provide clear and transparent information about how consumer data is collected, used, and stored. Consumers also have the right to opt out of the sale of their data to third parties, which is an important feature in protecting privacy in an increasingly connected digital environment. However, one of the main criticisms of the CCPA is the weak enforcement and inconsistency in the implementation of these regulations, which leads to uncertainty for consumers and companies alike.

Despite its weaknesses in terms of enforcement, the CCPA remains an important step in the protection of personal data in the United States, especially in providing consumers with basic rights to control their information. The regulation also inspired other states in the U.S. to develop similar data protection frameworks. At the international level, the CCPA demonstrates how a consumer-centric approach can provide better privacy protections, although there is a need for further strengthening in terms of law enforcement.

The Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada is one of the legal frameworks designed to protect personal data in the private sector. PIPEDA gives individuals the right to access and correct their personal data, ensuring that the information stored is accurate and up-to-date. In addition, these regulations require entities that manage personal data to provide notification in the event of a data breach, especially when the breach poses a risk to individuals. In the context of global data protection, PIPEDA has similarities with the European Union's General Data Protection Regulation (GDPR) and the Personal Data Protection Law (PDP Law) in Indonesia. However, the scope of PIPEDA is more limited because it focuses on the private sector, with relatively lighter enforcement power than GDPR (Fasken, 2022).

One of the strengths of PIPEDA is its flexibility in regulating the management of personal data in the private sector. These regulations allow companies to align their policies with established data protection principles, while still encouraging innovation and efficiency in data management. However, limitations in law enforcement are often a major challenge. Sanctions for violations under PIPEDA are not as severe as GDPR, so deterrent effects on violators are often considered inadequate. Nevertheless, PIPEDA remains an example of how data protection can be effectively implemented in the private sector while respecting the privacy rights of individuals.

In the Indonesian context, the PDP Law has similarities with PIPEDA in terms of granting access rights and data correction to individuals, as well as the obligation to notify data breaches. However, the PDP Law seeks to cover a wider range of sectors, including the public and private sectors, to create more holistic data protection. However, the level of law enforcement under the PDP Law also still needs to be strengthened. Lighter sanctions than GDPR create challenges in driving compliance, especially in the private sector, which often faces resource constraints and awareness of the importance of data protection.

To ensure the successful implementation of the PDP Law, Indonesia can take lessons from PIPEDA, especially in developing a flexible but still effective monitoring mechanism. A combination of a risk-based approach and consistent law enforcement can be a solution to improve data governance in the private sector. In addition, educating companies about the importance of data protection and its impact on consumer trust needs to be a priority. Thus, the PDP Law can be a framework that is not only in line with global standards such as GDPR but also relevant to local needs in Indonesia.

Article 4 Paragraph (2) of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) emphasizes the importance of basic principles that must be applied by Electronic System Operators (PSEs) in managing sensitive data. These principles include transparency, security, and accountability, which are designed to protect individual privacy and ensure that sensitive data is processed ethically and in accordance with the law. These three principles are the main cornerstones in the management of

sensitive data, reflecting the regulatory commitment to provide adequate protection against evolving threats in the digital era.

The principle of transparency requires PSEs to provide clear and easily accessible information to the public about how sensitive data is collected, processed, and used. This information should include the purpose for which the data was collected, the types of data being managed, and the parties to whom the data was given access. This transparency aims to build trust between PSEs and data subjects, ensuring that individuals understand how their personal information is being used. In this context, transparency is not only a legal obligation but also an important mechanism to increase accountability and public trust in data management.

The security principle emphasizes the obligation of PSEs to protect sensitive data from unauthorized access and potential breaches. This includes the implementation of security technologies such as data encryption, double authentication, and risk-based monitoring systems to prevent data leakage or misuse. In an increasingly complex digital world, where cyber threats are on the rise, these security principles are key to ensuring the integrity of sensitive data. Additionally, security measures should be updated regularly to deal with new threats that may emerge.

The principle of accountability requires PSEs to be responsible for the management and processing of sensitive data. PSE is required to ensure that the data management process is carried out in accordance with applicable regulations and to protect data through regular audits. These audits aim to identify weaknesses in the data management system and ensure that corrective measures are implemented effectively. Accountability also includes the responsibility to report incidents of data breaches to the authorities and data subjects within the time set by the PDP Law.

These three principles complement each other and form a comprehensive framework for the protection of sensitive data. Consistent implementation of transparency, security, and accountability principles can help reduce the risk of data breaches, increase public trust, and support a secure and trusted digital ecosystem. In a global context, these principles are also in line with international frameworks such as the General Data Protection Regulation (GDPR), which makes the PDP Law relevant in data governance in the era of globalization. However, the successful implementation of these principles relies heavily on strict supervision, education to PSEs, and consistent law enforcement.

Thus, Article 4 Paragraph (2) of the PDP Law not only provides guidance for PSEs in managing sensitive data but also reflects the Indonesian government's efforts to create comprehensive and adaptive data protection regulations for technological developments.

The implementation of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) in Indonesia faces a number of significant challenges, which hinder the effectiveness of personal data protection in the digital era. One of the main challenges is the lack of adequate resources, both in terms of technological infrastructure and a trained workforce. Many Electronic System Operators (PSEs), especially those operating on a small and medium scale, do not have the capacity to meet the data protection standards mandated by the PDP Law. Technologies such as data encryption and double authentication, which are critical components in keeping data secure, are often not implemented consistently. This makes personal data, especially sensitive data, vulnerable to leakage and misuse.

In addition, uncertainty in the implementation of regulations is also an obstacle. Some provisions in the PDP Law require more detailed technical guidelines to ensure that PSEs can understand and meet legal requirements effectively. This uncertainty creates a gap between existing regulations and their implementation on the ground. As a result, data breaches continue to occur, even though legal frameworks are in place. Data leakage incidents involving individual personal information, such as health, financial, or biometric data, indicate that the protection measures in place are still inadequate.

To overcome this problem, strengthening supervision and law enforcement is an urgent need. The government needs to ensure that the implementation of the PDP Law is closely monitored through a regular audit mechanism of PSE. These audits not only aim to monitor compliance but also to identify weaknesses in the data management system so that they can be corrected before a breach occurs. In addition, consistent law enforcement with strict sanctions against violations needs to be implemented to

provide a deterrent effect. This enforcement should include significant fines or operational cessation for PSEs that fail to comply with data protection provisions.

Education and training are also an important step to increase understanding among PSEs about their obligations under the PDP Law. Governments and the private sector need to work together to provide training programs that cover best practices in data management, the use of security technologies, and the fulfillment of transparency, security, and accountability principles. Thus, the implementation of the PDP Law can be more effective in protecting people's personal data, creating a safer digital ecosystem, and building public trust in data governance in Indonesia.

The challenges in implementing the PDP Law reflect the complexity of data protection in the digital era. However, by strengthening regulations, supervision, and cross-sector collaboration, Indonesia can present a more resilient and adaptive personal data protection system to technological changes.

The implementation of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) faces various challenges, especially for Electronic System Operators (PSE) who are one of the main actors in personal data management. One of the main obstacles is the lack of trained human resources in data management and the application of adequate security technology. Many PSEs do not yet have staff who have the specific competencies to understand and implement data protection principles, such as transparency, security, and accountability. The lack of training and education related to data governance makes it difficult to meet the protection standards mandated by the PDP Law.

In addition, the limitation of technological resources is a significant obstacle. Many PSEs, especially those operating on a small and medium-sized scale, do not have the necessary technological infrastructure to meet data protection requirements. Technologies such as encryption, double authentication, or risk-based monitoring systems, which are critical elements in keeping personal data safe, are often not available or implemented effectively. The inability to access this technology makes the personal data they manage vulnerable to security threats, such as hacking or data leaks.

Another factor that has exacerbated the situation is the lack of awareness among PSEs of the importance of protecting personal data. Some PSEs see compliance with the PDP Law as an additional administrative burden, without understanding that data protection is not only a legal obligation but also an investment in building public trust. This lack of awareness often leads to a lack of priority on data management that is secure and in accordance with regulatory standards.

The combination of these constraints creates a significant gap between the provisions regulated in the PDP Law and data management practices in the field. To overcome these obstacles, a collective effort from the government, the private sector, and the community is needed. The government needs to provide support in the form of training and certification programs to increase the capacity of human resources in PSE. In addition, incentives can be provided to encourage the adoption of security technologies, especially for small-scale PSEs that often face budget constraints.

Ongoing education on the importance of protecting personal data is also needed to raise awareness among PSEs about the long-term benefits of regulatory compliance. With these steps, PSEs can be better prepared to face challenges and meet the data protection standards mandated by the PDP Law, while increasing public trust in data governance in Indonesia.

Technological advancements offer innovative solutions to overcome challenges in personal data protection. Technologies such as artificial intelligence (AI), blockchain, and advanced encryption methods can play a key role in improving data security and protecting individual privacy. AI, for example, can be used to detect security threats in real-time by analyzing anomalous patterns in systems that indicate potential hacks or data breaches. Blockchain technology, with its decentralized structure, provides a secure and transparent data storage mechanism, minimizing the risk of data manipulation by unauthorized parties. Meanwhile, advanced encryption methods ensure that sensitive data transmitted or stored can only be accessed by authorized authorities, thus preventing unauthorized access.

However, the application of this technology cannot stand alone without a solid policy framework and collaboration between the government and Electronic System Operators (PSEs). Governments have an important role to play in formulating policies that support the adoption of these security technologies, including establishing clear technical standards and providing incentives for PSEs to adopt cutting-edge

technologies. On the other hand, PSEs must be proactive in integrating this technology into their data management systems, while also ensuring that their staff has the necessary knowledge and skills to manage it.

Collaboration between the government and PSE should also include efforts to raise awareness about the importance of personal data protection. Ongoing education campaigns can help change the perception that data protection is just an administrative burden into a strategic investment to build public trust. In addition, strict law enforcement against data protection violations is an important element in ensuring compliance. Clear and consistent sanctions not only provide a deterrent effect but also demonstrate a serious commitment to protecting individual privacy.

The implementation of advanced technology in data protection must be complemented by continuous supervision and evaluation. This is important to ensure that the technology used remains relevant to the evolving development of security threats. By combining advanced technology, effective policies, and cross-sector collaboration, personal data protection in Indonesia can be significantly improved, creating a safe and reliable digital ecosystem.

CONCLUSION

Personal data protection in the digital era is an issue that is increasingly relevant with increasing threats to individual privacy and information security. Through Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), Indonesia has demonstrated its commitment to building a legal framework that protects the right to privacy and ensures more responsible management of personal data. However, the implementation of this law is inseparable from significant challenges, including limited technological resources, low awareness among Electronic System Operators (PSEs), and weaknesses in law enforcement.

Basic principles such as transparency, security, and accountability regulated in the PDP Law are the main pillars to protect personal data, especially sensitive data. The implementation of these principles requires synergy between the government, PSE, and the community. The government should take an active role in providing clear technical guidelines, strengthening oversight mechanisms, and providing strict sanctions for violations. On the other hand, PSEs must increase their human resource capacity and adopt advanced security technologies such as AI, blockchain, and encryption to minimize the risk of data leaks.

In a global context, the PDP Law is aligned with international data protection standards such as the European Union's General Data Protection Regulation (GDPR). However, there are still differences in the level of law enforcement and the amount of sanctions that can reduce the deterrent effect of violations. Lessons learned from regulations such as GDPR and PIPEDA in Canada can help Indonesia strengthen law enforcement and improve data protection efficiency at the national level.

The role of the community is also very important in the successful implementation of the PDP Law. Public education on the importance of protecting personal data can increase individuals' awareness of their rights, encourage compliance with data management principles, and reduce potential data exploitation. Ongoing awareness campaigns can change people's perception that data protection is a fundamental need, not just an administrative obligation.

By overcoming existing challenges, Indonesia has a great opportunity to create a safe and reliable digital ecosystem. Strategic measures such as strengthening regulations, implementing advanced technology, increasing PSE capacity, and educating the public must be implemented synergistically to ensure the effective protection of personal data. Ultimately, the successful implementation of the PDP Law will not only protect individual privacy but also strengthen public trust in data governance and support the sustainable development of the digital economy.

REFERENCE

California Department of Justice. (2020). *California Consumer Privacy Act (CCPA): Overview and implementation*. DOJ.

California Consumer Privacy Act. (2020). *Regulation text and guidelines*. DOJ.

DLI Tech. (2021, December 7). The promise and pitfalls of the California Consumer Privacy Act. *Cornell Tech*. https://www.dli.tech.cornell.edu/post/the-promise-and-pitfalls-of-the-california-consumer-privacy-act

European Union. (2018). *General Data Protection Regulation (GDPR)*. Official Journal of the European Union.

Fasken. (2022, July 26). Comparative table of personal information protection laws. https://www.fasken.com/en/knowledge/2022/07/26-comparative-table-of-personal-information-protection-laws

Hukumonline. (2023, November 2). UU PDP: Pelaksanaan kewajiban pengendali dan prosesor data pribadi jadi tantangan. https://www.hukumonline.com/berita/a/uu-pdp--pelaksanaan-kewajiban-pengendali-dan-prosesor-data-pribadi-jadi-tantangan-lt63689b9f8a255

Indonesia.go.id. (2021, September 24). Era baru perlindungan data pribadi. https://indonesia.go.id/kategori/editorial/8725/era-baru-perlindungan-data-pribadi?lang=1

Kominfo. (n.d.). Perlindungan data pribadi di Indonesia: Tantangan dan solusi untuk masa depan. *Jurnal Iptek Komunikasi, 17*(2). https://jurnal.kominfo.go.id/index.php/iptekkom/article/download/3505/1477/12301

Komnas HAM. (2021, July 16). Kajian RUU Perlindungan Data Pribadi dalam perspektif HAM. https://www.komnasham.go.id/index.php/news/2021/7/16/1846/kajian-ruu-perlindungan-data-pribadi-dalam-perspektif-ham.html

Marzuki, P. M. (2017). *Penelitian hukum: Edisi revisi*. Kencana Prenada Media Group.

Miller, C. (2023, May 15). How blockchain is transforming data security. *TechCrunch*. https://techcrunch.com/2023/05/15/how-blockchain-is-transforming-data-security

Ombudsman Republik Indonesia. (2021). *Laporan tahunan Ombudsman Republik Indonesia: Kepercayaan publik dan perlindungan data pribadi*. Ombudsman RI.

PinterPandai. (n.d.). Perlindungan data pribadi: UU PDP di Indonesia, pemahaman GDPR, persyaratan, konsekuensi, dan contoh. Retrieved December 5, 2024, from https://www.pinterpandai.com/perlindungan-data-pribadi-uu-pdp-di-indonesia-pemahaman-gdpr-persyaratan-konsekuensi-dan-contoh

Privy.id. (2021, February 8). Pentingnya menjaga keamanan data pribadi. *Privy Blog*. Retrieved December 5, 2024, from https://blog.privy.id/pentingnya-menjaga-keamanan-data-pribadi/

Puskomedia. (n.d.). Mengamankan data pelanggan: Praktik terbaik untuk perlindungan data sensitif. Retrieved December 5, 2024, from https://www.puskomedia.id/blog/mengamankan-data-pelanggan-praktik-terbaik-untuk-perlindungan-data-sensitif/

Rahayu. I. L., Syarifa. R., Akmalia. L. R., Samosir. M. S., Hanggrita. E. P., Muflikhati. I., & Simanjuntak. M. (2023). Willingness to share data pribadi dan kaitannya dengan penyalagunaan data konsumen e-commerce di Indonesia: Pendekatan mixed methods. *Jurnal Ilmiah Keluarga & Konsumen*, 16(3), 274–287. https://doi.org/10.24156/jikk.2023.16.3.274

Salim, H. S., & Nurbani, E. S. (2013). *Penerapan teori hukum pada penelitian tesis dan disertasi*. RajaGrafindo Persada.

Simbolon, V. A., & Juwono, V. (2022). Comparative review of personal data protection policy in Indonesia and the European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi)*, 11(2), 178–190. https://doi.org/10.31314/pjia.11.2.178-190

Smith, J. (2024, December 5). How AI is changing data security. *TechCrunch*. https://techcrunch.com/article-url

Sugiyono. (2016). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.

Sustain Indonesia. (2024, January 16). Empat perbuatan yang dilarang dan sanksinya berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP). Retrieved December 5, 2024, from https://sustain.id/2024/01/16/empat-perbuatan-yang-dilarang-dan-sanksinya-berdasarkan-undang-undang-nomor-27-tahun-2022-tentang-pelindungan-data-pribadi-uu-pdp/

Tari Oktaviani, & Nailufar, N. N. (2023, July 19). UU Perlindungan Data Pribadi: Jenis data dan sanksi pidananya. *Kompas.com*. https://nasional.kompas.com/read/2023/07/19/00150031/uu-perlindungan-data-pribadi-jenis-data-dan-sanksi-pidananya

Tirto.id. (2022, October 17). Isi UU Perlindungan Data Pribadi: Undang-Undang No. 27 Tahun 2022. *Tirto*. https://tirto.id/isi-uu-perlindungan-data-pribadi-undang-undang-no-27-tahun-2022-gFk7

Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Yum, M. (2018). About the distribution of wealth and jobs. *Economic Dynamics Review, 30*, 86–105.