The Challenges of Implementing the Personal Data Protection Law in Indonesia: Delays in Establishing a Regulatory Authority

Bhimo Aji Hernowo

{Hernowobhimo@gmail.com }

Borobudur University

Abstract. Indonesia is facing a significant problem related to serious personal data leaks. To overcome this problem, the Personal Data Protection Law (Law No. 27 of 2022) was passed. However, its role and function are still a matter of debate. According to the law, this authority is tasked with formulating and establishing PDP policies and strategies, which will serve as guidelines for Personal Data Subjects, Data Controllers and Data Processors. The Authority is also responsible for monitoring the implementation of the PDP, enforcing administrative laws, and facilitating the resolution of disputes regarding personal data. However, to date, this regulatory authority has not been established, neither a Presidential Decree nor a Government Regulation (PP) which further explains the function and authority of this authority has been determined. Implementation of the Personal Data Protection Law in Indonesia continues to face serious challenges in the form of the slow establishment of this important regulatory authority.

Keywords: Personal Data Protection, Regulatory Authority, Personal Data Leakage

1 Intoductions

The rapidly advancing pace of information technology presents new opportunities and challenges. The evolution of information technology has interconnected humans on a broader scale, transcending geographical boundaries. The escalating development of information technology is harnessed across various sectors, including trade, education, electronic governance, healthcare, and others. The utilization of information technology in these sectors facilitates the easy collection and transfer of an individual's personal data without the knowledge of the data owner. This scenario poses a threat to the security of personal data.

ICL-C 2023, November 11, Jakarta, Indonesia

DOI 10.4108/eai.11-11-2023.2351333

The ease with which personal data becomes readily available and transferable in the realm of information technology poses a potential threat to the security of personal data. In light of the risks and threats posed by information technology on the security of personal data, there is a need for instruments to safeguard such personal data. These instruments are expected to have the capability to protect both the information contained in personal data and the individuals themselves.[1]

The development of technology and the internet has become a crucial factor complicating the dynamics of personal data protection. According to a survey by the Association of Indonesian Internet Service Providers (APJII), the number of internet users in Indonesia reached 215.63 million people (78.19% of the total population) during the 2022-2023 period.[2] With the increasing number of internet users in Indonesia, the use of technology has become more pervasive in various aspects of community life. Although the collection of personal data has become commonplace, it is not accompanied by adequate security guarantees, as evidenced by the ongoing prevalence of data breaches.

Data breaches continue to be prevalent. In the e-commerce sector, for instance, Tokopedia experienced a data breach affecting 91 million user accounts and 7 million seller accounts in April 2020. This breach, orchestrated by a hacker, encompassed email addresses, passwords, and usernames. [3] The banking sector has also faced data breach incidents. In January 2022, Bank Indonesia fell victim to a cyberattack by a hacker from Russia. The perpetrators obtained documents from computers within Bank Indonesia, totaling 74 gigabytes from 237 computers in the bank's network.[4]

The leakage of personal identities, which should be safeguarded, creates vulnerabilities to the risks of fraud and information misuse. This issue is not only of sociological concern but also a legal imperative to establish regulations governing the protection of personal data.[5] The prevalent phenomenon of personal data theft, exemplified by incidents such as those instigated by Bjorka, underscores the urgency of an integrated regulatory authority to address these threats.

Personal data can be categorized into two types: specific personal data and general personal data. Specific personal data, such as biometric and genetic information, has a profound impact on the individuals it pertains to, while general personal data, including full names, religion, and citizenship, is more commonplace. The collection of this data in electronic systems carries the risk of leaks due to hacking, poor governance, human resource quality in information systems, and the obsolescence of the technology used. [6]

The need for personal data protection is increasingly pressing in this digital era, aligning with the fundamental rights of every individual recognized in Article 28G of the 1945 Constitution, which asserts the right to personal protection. While the Constitution does not explicitly mention the right to privacy, the norms contained in Article 28G provide a strong constitutional basis for the state to safeguard privacy through personal data protection (PDP).[7]

Personal data protection is not just a national issue but also part of international responsibility. The concept of the right to privacy as a part of Human Rights emphasizes the necessity of protecting privacy as an effort to create justice, certainty, and legal benefits.[8] The government responded by issuing Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), which places special emphasis on institutionalization as a primary pillar of its implementation.

As of now, there is no comprehensive regulatory authority overseeing personal data protection. Often, authority are established only after the issuance of regulations, leading to legal uncertainty that impacts the values of certainty, justice, and utility. PDP supervision remains sectoral, with entities like the Financial Services Institution (OJK) overseeing the banking sector and the Ministry of Communication and Informatics (Kominfo) overseeing other sectors such as telecommunications. Data breaches not only occur in specific sectors but also extend to e-commerce, the Social Security Administering Body (BPJS), and government programs such as PeduliLindungi. In the context of PDP supervision, Chapter IX of the PDP Law addresses authority as key instruments in maintaining the security and privacy of personal data. The presence

of regulatory authority becomes crucial to address legal uncertainties that may hinder the values of certainty, justice, and utility.

2 Method

This research employs a normative legal research design, specifically adopting the Library Research approach. This method involves the collection of data from various literature sources relevant to the research issue. Secondary data sources include legal materials such as court decisions and textbooks covering fundamental principles in legal science, as well as classical views from renowned scholars. The literature review entails a thorough examination of books, literature, notes, and reports related to the raised issue. [9] This research utilizes a conceptual approach, combining the scientific insights of legal science with legal theory to examine relevant issues. The conceptual framework is rooted in views and doctrines that have evolved in the field of legal science. Through the exploration of these views and doctrines, the author clarifies ideas that contribute to the formation of understanding, concepts, and legal principles relevant to the researched issue. The methodological approach adopted in this research is legislative, specifically referring to Law Number 27 of 2022 concerning Personal Data Protection.

3 Results And Discussion

The increase in complaints regarding the misuse of personal data received by the Jakarta Legal Aid Institute (LBH) rose by 143% during the second quarter of 2022. Data breaches were also experienced by users who input their information into Pertamina's database, where 44 million user data was sold by hackers for 392 million rupiahs. In the same year, user data from the State Electricity Company (PLN) was obtained, with 17 million user data scattered in hackers' forums, including names, addresses, and bills. The persistence of data breaches implies that the enacted Personal Data Protection Law (PDP Law) has yet to fully meet the privacy rights of the public. [10]

The protection of personal data is embedded within the framework of human rights. Personal data protection safeguards basic human rights, as stated in Article 28G(1) of the 1945 Constitution of

the Republic of Indonesia, which asserts that "Every person has the right to protection of oneself, family, honor, dignity, and property under their control, as well as the right to security and protection from threats of fear to do or not to do something that is a human right." According to Article 1 Number 1 of the PDP Law, personal data refers to data about individual persons that are identified or can be identified either individually or in combination with other information, directly or indirectly, through electronic or non-electronic systems. Meanwhile, Article 1 Number 2 defines personal data protection as the overall efforts to protect personal data within the series of personal data processing to guarantee the constitutional rights of the personal data subject.[6]

The continually advancing information technology across various sectors and international boundaries exposes personal data associated with such technology to easy dissemination and uncertain security. Therefore, instruments are needed to provide protection for this personal data. The protection of personal data can facilitate transnational trade, industry, and investment.

The PDP Law regulates the rights of personal data owners, known as personal data subjects. Personal data subjects have the right to:[6]

1. Obtain information about the clarity of identity, legal basis, purposes of the request, and use of personal data, as well as the accountability of the party requesting personal data.
2. Complete, update, and/or correct errors and/or inaccuracies in personal data about themselves in accordance with the purpose of personal data processing.
3. Access and obtain copies of personal data about themselves in accordance with the provisions of laws and regulations.
4. Terminate processing, delete, and/or destroy personal data about themselves in accordance with the provisions of laws and regulations.
5. Withdraw consent for the processing of personal data about themselves given to the personal data controller.
6. Object to decisions based solely on automated processing, including profiling, that have legal consequences or significant impacts on personal data subjects.

7. Temporarily or restrictively process personal data in proportion to the purpose of personal data processing.
8. Obtain and/or use personal data about themselves from the personal data controller in a format commonly used or readable by electronic systems.

Several rights of personal data subjects can only be applied after submitting a recorded request electronically or non-electronically to the personal data controller. Personal data rights may be exempted in cases of:

1. National defense and security interests.
2. Law enforcement process interests.
3. Public interests in the context of state administration.
4. Interests in the supervision of financial services, monetary, payment systems, and financial system stability conducted in the context of state administration.
5. Statistical and scientific research interests.

The PDP Law also regulates the entities controlling personal data processing. The controlling party can be individuals, public entities, and international organizations acting independently or together. In carrying out their duties, personal data controllers must have a legal basis for processing personal data. This basis may be consent from the personal data subject, compliance with legal obligations, public interests, public services, and others.

According to the PDP Law, in the event of a failure in personal data protection, the personal data controller must provide written notification within 3 x 24 (three times twenty-four) hours to:

1. Personal data subjects; and
2. Authorities.

Personal data protection is not just about safeguarding personal information through equivalent legal mechanisms. Another critical aspect is the establishment of an authority responsible for personal data protection. To date, supervision of personal data protection remains sectoral, depending on the authority granted by regulations governing such personal data. While sectoral supervision may lead to debates and overlapping authorities among various authoritys.[11]

The PDP Law states that the government plays a role in implementing personal data protection. The implementation of personal data protection is carried out by an authority designated by the President and accountable to the President. The authority overseeing personal data protection performs tasks such as:[6]

1. Formulating and establishing policies and strategies for personal data protection that serve as guidance for personal data subjects, personal data controllers, and personal data processors.
2. Supervising the implementation of personal data protection.
3. Enforcing administrative law against violations of this law.
4. Facilitating dispute resolution outside of court..

Additionally, the authority responsible for personal data protection is empowered to:

1. Formulate and establish policies in the field of personal data protection.
2. Supervise compliance with personal data controllers.
3. Impose administrative sanctions for violations of personal data protection committed by personal data controllers and/or personal data processors.
4. Assist law enforcement authorities in handling allegations of personal data offenses as defined in this law.
5. Collaborate with data protection agencies in other countries to resolve allegations of cross-border violations of personal data protection.
6. Assess compliance with requirements for transferring personal data beyond the legal jurisdiction of the Republic of Indonesia.
7. Issue orders for follow-up actions based on the results of supervision to personal data controllers and/or personal data processors.
8. Publish the results of personal data protection supervision in accordance with the provisions of laws and regulations.
9. Receive complaints and/or reports regarding alleged violations of personal data protection.
10. Conduct examinations and investigations into complaints, reports, and/or the results of supervision regarding alleged violations of personal data protection.

11. Summon and bring in any individual and/or public entity related to allegations of violations of personal data protection.
12. Request statements, data, information, and documents from any individual and/or public entity related to allegations of violations of personal data protection.
13. Summon and bring in experts as needed in examinations and investigations related to allegations of violations of personal data protection.
14. Conduct examinations and investigations into electronic systems, facilities, spaces, and/or places used by personal data controllers and/or personal data processors, including obtaining access to data and/or appointing third parties.
15. Seek legal assistance from the prosecution in resolving disputes related to personal data protection..

Based on the aforementioned provisions, it can be concluded that the authority responsible for personal data protection has extensive authority. The authority is authorized to formulate and establish policies in the field of personal data protection. Moreover, the authority has the power to supervise the compliance of personal data controllers and can impose administrative sanctions for violations. Additionally, the authority can assist law enforcement authorities in addressing alleged criminal offenses related to personal data. It is also empowered to collaborate internationally to resolve cross-border violations and assess compliance with data transfer requirements..[6]

Further regulations regarding the authority responsible for personal data protection will be stipulated by the Presidential Regulation. The transitional provisions of the Personal Data Protection Law state that parties involved in personal data processing must align with the provisions within two years of the law's enactment on October 17, 2022. Accordingly, the authority for personal data protection should ideally be established before October 2024. Considering the broad tasks of the authority, it is expected to provide legal certainty for personal data protection beyond the law itself.[6]

Although the Personal Data Protection Law has addressed the needs of society by addressing the diversity of personal data protection in sectoral regulations, the aspect of legal certainty is still unmet. Therefore, an overseeing authority is necessary as a guarantee for the security of personal data in society. Based on the explanations in the Personal Data Protection Law, the role of the authority is crucial for the implementation of the law. However, there are still some points not discussed regarding the authorityal oversight of personal data protection, including:[10], [12]

1. Name and Form of the Authority:

   The Personal Data Protection Law does not specify the name and form of the authority overseeing personal data protection. This is different from independent commissions such as the Indonesian Child Protection Commission (KPAI) and autonomous authoritys like the Witness and Victim Protection Agency (LPSK). The law only mentions that the authority will be determined by the president. Nevertheless, it must be ensured that the authority to be established is independent to achieve justice, objectivity, and prevent political interference. Independence does not mean without supervision. Internal oversight by the authority can still be carried out to minimize interference. Several other countries have established independent authoritys overseeing personal data protection, such as France with the Commission Nationale de l'informatique et des Libertés (CNIL). However, many ASEAN countries do not have independent oversight since their focus is only on private data controllers.

2. Maximum Timeframe for Authority Formation:

   The establishment of other authoritys regulated by law usually includes a maximum timeframe for the formation of the authority. Although there are no specified sanctions for delays in establishment and no assurance of timely formation, this provision can give the public an indication of when the authority will be formed, and the public can hold the government accountable for its commitment.

The absence of these elements indicates a lack of readiness in the design and enforcement of laws, making them binding for the community and obscuring the legal objectives in terms of legal

certainty. Nevertheless, there are several factors driving the prompt establishment of a Personal Data Protection (PDP) oversight authority in Indonesia, including: [12], [13]

1. Ensuring the Implementation of PDP Law Regulations

   The PDP Law has outlined the tasks, functions, and power of the PDP oversight authority to monitor the implementation of PDP.

2. Oversight and Enforcement of PDP Law that is Sectoral and Weak

   Sectoral-based PDP oversight is still insufficient to effectively monitor and enforce the law. This is because there is no comprehensive PDP oversight. Additionally, there may be overlaps in the power and functions of the PDP authority with other authoritys engaged in data processing activities.

3. Numerous Legal Subjects in PDP

   As previously mentioned, the majority of the Indonesian population is already using the internet. Supervising the public's internet usage is challenging, especially in terms of PDP, where the public is highly vulnerable to the dissemination or theft of personal data.

4. Many Public, Private, Individual, and International Organizations as Personal Data Controllers

   According to the PDP Law, data controllers or processors can vary widely. The existence of a PDP oversight authority can ensure that data controllers comply with the PDP Law or other derivative regulations set by the PDP oversight authority while processing data by determining the level of security for the protection of such data.

5. Limited Public Knowledge and Awareness of PDP

   The weak awareness is demonstrated by the ease with which the public fills out online forms, uploads personal data on social media, or simply agrees to the terms of service of a website or application without understanding the impact on their personal data. The presence of a PDP oversight authority is expected to prevent data leaks from occurring at the source. The public can be educated about the possibility of personal data misuse and how to be more cautious in utilizing the latest technological developments.

4 Conclusion

The enactment of the PDP Law addresses the current needs of society and aligns with the evolving times, reflecting the principle of responsive law. However, the absence of the authority raises doubts regarding the principle of legal certainty, as the envisaged authority is tasked with executing the regulations. Therefore, it is imperative to promptly formulate detailed provisions in the form of Government Regulations, serving as the legal framework for the establishment of the PDP oversight authority. These regulations will address authorityal aspects not explicitly outlined in the PDP Law and further delineate the authority's tasks, functions, and power in overseeing and enforcing PDP laws.

References

[1] M. B. Yel and M. K. M. Nasution, "Keamanan Informasi Data Pribadi Pada Media Sosial," *J. Inform. Kaputama*, vol. 6, no. 1, pp. 92–101, 2022, doi: 10.59697/jik.v6i1.144.

[2] M. R. Kandau and Munawaroh, "Pengaruh Penggunaan Media Sosial Dan Differentiation Produk Terhadap Keputusan Pembelian Pada Erni Dimsum Di Medan Johor," *J. Inov. Penelitia*, vol. 4, no. 2, pp. 547–554, 2008.

[3] M. Raihan, "Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia)," *J. Inov. Penelit.*, vol. 3, no. 10, pp. 7847–7856, 2023.

[4] A. C. Kusuma and A. D. Rahmani, "Analisis Yuridis Kebocoran Data Pada Sistem Perbankan Di Indonesia (Studi Kasus Kebocoran Data Pada Bank Indonesia) Aditama Candra Kusuma , Ayu Diah Rahmani Fakultas Hukum , Universitas Pembangunan Veteran Jakarta Kemajuan teknologi sangat membantu manu," *J. Huk.*, vol. 5, no. 01, pp. 46–63, 2022.

[5] A. Soraja, "Perlindungan Hukum Atas Hak Privasi dan Data Pribadi dalam Prespektif HAM," *Pros. Semin. Nas. Kota Ramah Hak Asasi Mns.*, pp. 20–32, 2021.

[6] Pemerintah Republik Indonesia, *Undang-Undang No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi*. 2022.

[7] Pemerintah Republik Indonesia, *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*, vol. 23. 2017, p. 1. [Online]. Available: https://www.mpr.go.id/img/sosialisasi/file/1610334013_file_mpr.pdf

[8] R. Natamiharja and S. Mindoria, "Perlindungan Hukum Atas Data Pribadi Di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi Pt. Telekomunikasi Selular) Legal Protection of Personal Data in Indonesia (Study of the Implementation of Telecommunications Services At Pt. Telek," 2019.

[9] D. L. Sonata, "METODE PENELITIAN HUKUM NORMATIF DAN EMPIRIS: KARAKTERISTIK KHAS DARI METODE MENELITI HUKUM," vol. 8, no. 1, pp. 15–35, 2014.

[10] E. Yolanda and R. R. Hutabarat, "Urgensi Lembaga Pelindungan Data Pribadi di Indonesia Berdasarkan Asas Hukum Responsif," *J. Eng. Res.*, vol. 8, no. 6, 2023, doi: 10.36418/syntax-literate.v6i6.

[11] E. S. Ayuningtyas, "Urgensi Pembentukan Lembaga Perlindungan Data Pribadi Dalam Uu No. 27 Tahun 2022 Tentang Pelindungan Data Pribadi Perspektif Hukum Positif Dan Hukum Islam.pdf," Universitas Islam negeri Prof KH. Saifuddin Zuhri Purwokerto, 2023.

[12] R. Pratama and E. R. Wulan, "Urgensitas Pembentukan Lembaga Penyelenggaraan Pelindungan Data Pribadi," *Bur. J. Indones. J. Law Soc. Gov.*, vol. 3, no. 2, pp. 1828–1845, 2023.

[13] D. Doly, "Pembentukan Lembaga Pengawas Pelindungan Data Pribadi dalam Perspektif Pembentukan Lembaga Negara Baru," *Negara Huk.*, vol. 12, no. 2, p. 227, 2021.