Law Synergy Conference (LSC)
Volume I; Number I; Month 6, Year 2024; Pages 209-215
Website:https://sinergilp.com
E-ISSN: 3048-3530

Legal Protection of Personal Data in the Digital Era

Rudianto Sahnitra Padang[1], T. Riza Zarzani[2].
Rudipadang90@gmail.com rizazarzani@dosen.pancabudi.ac.id
[12]Panca Budi Development University

Abstract

The ever-evolving digital era brings new challenges in personal data protection, which requires an improvement in the legal framework in Indonesia. This study aims to analyze the weaknesses of Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, and to find solutions to improve the effectiveness of personal data protection in the context of globalization and digital interconnection. The method used is normative juridical with a comparative approach, reviewing applicable laws and comparing them with international regulations such as GDPR. The results of the study indicate that there is an urgent need for a clearer definition, the establishment of an independent supervisory authority, and the integration of international standards to strengthen the legal framework for personal data protection in Indonesia. Recommendations provided include dynamic and responsive legislative reform, increasing digital literacy, and building secure infrastructure.

Keywords:*Personal Data Protection, Legal Reform, International Standards*

INTRODUCTION

In this digital era of interconnectedness, the exponential growth of data and information has changed the paradigm of social interaction and economic transactions globally. Advances in information technology enable individuals and companies to collect, store, and process large amounts of data at high speed and relatively low cost. However, this development also poses significant challenges in terms of personal data protection. The issue of personal data protection has become a major concern in many countries, including Indonesia, which faces challenges in developing an effective legal framework to address the problem of personal data leakage and misuse.

In the Indonesian context, the urgency of personal data protection is underscored by a series of data breach incidents that highlight the vulnerability of information systems and the failure of existing protection mechanisms. According to Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) as amended by Law Number 19 of 2016, personal data protection is regulated in several articles that include provisions on electronic transactions and electronic information whose confidentiality must be protected. However, existing regulations are often inadequate to address the dynamics and new risks that arise from the use of ever-evolving digital technology.

Meanwhile, the interaction between technology and privacy continues to evolve, making personal data protection not only a technical issue, but also an ethical and legal one. The inadequacy of the current legal framework in addressing new issues related to personal data raises an urgent need for a review and update of existing regulations. In order to strengthen personal data protection, the Indonesian government has begun taking steps to develop a specific law governing personal data protection, which is expected to provide a more comprehensive and adaptive legal framework to technological changes. What are the weaknesses of the current legal framework governing personal

data protection in Indonesia in facing the challenges of the digital era? This analysis will explore the inadequacies of Law Number 11 of 2008 and its amendments in addressing the issue of personal data security and privacy, taking into account the dynamics of rapidly changing technology and data breach incidents that have occurred.

How can Indonesia improve its legal framework to ensure effective personal data protection in the context of globalization and digital interconnection? This question aims to explore regulatory and policy options that Indonesia can adopt to strengthen personal data protection, including considering international best practices and adapting policies to suit Indonesia's socio-economic context.

In the context of Indonesian law, the ITE Law has become the legal basis governing electronic transactions, including aspects of personal data protection. According to Article 26 of the ITE Law, every person who has personal data in an electronic system has the right to request protection of his/her personal data. This article underlines the individual's right to privacy of data and personal information collected and stored in an electronic system. However, this article does not explicitly mention the implementation mechanism and sanctions for violations, which makes it less effective in its implementation (Law Number 11 of 2008).

Referring to the existing legal framework, there is a need for a review and update that can strengthen personal data protection by considering several aspects, such as a clearer definition of personal data, stricter monitoring mechanisms, and adequate sanctions for violations that occur. This study will use a comparative analysis approach, examining the comparison between Indonesian regulations and regulations from other countries that already have more advanced personal data protection laws.

METHOD

This study uses a normative legal research method that aims to examine and analyze the applicable legal framework, especially related to personal data protection in the Indonesian context. This methodology involves collecting secondary data through literature studies that include legislation, books, journal articles, and other official documents that are relevant to the legal issues being studied. In addition, a comparative study will be conducted to compare personal data protection regulations in Indonesia with other countries that already have mature regulations in this field, such as the European Union with its General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679).

Data analysis will be conducted descriptively analytically, where data obtained from legal sources will be interpreted to determine the adequacy and effectiveness of current personal data protection and identify existing gaps. The results of this analysis are expected to provide concrete recommendations related to the improvement of existing laws or the formulation of new laws that are more adaptive to the development of digital technology (Smith, 2020).

RESULTS AND DISCUSSION

Analysis of Weaknesses of the Legal Framework for Personal Data Protection in Indonesia

Amidst the increasingly intensive acceleration of digitalization, the issue of personal data protection has become a very important topic, especially in Indonesia. Law Number 11 of 2008

concerning Electronic Information and Transactions (UU ITE), as amended by Law Number 19 of 2016, is the main legal umbrella governing personal data protection in Indonesia. Although this regulation is a good first step, there are several significant weaknesses that need to be considered, especially in facing the challenges of the rapidly changing digital era.

One of the main weaknesses of the ITE Law is the lack of a clear and comprehensive definition of personal data. The ITE Law does not explicitly define what is meant by personal data, which has the potential to cause legal uncertainty and difficulties in its implementation (Satrio, 2018). Without a clear definition, it is very difficult to determine the scope of data protection and distinguish the types of data that must be protected. This also causes difficulties in determining the obligations of stakeholders in managing personal data.

Furthermore, the ITE Law provides ample room for the government to conduct wiretapping and surveillance of electronic transactions without adequate control from check and balance mechanisms. Although Article 31 paragraph (4) of the ITE Law requires court approval for wiretapping, the absence of a strong independent oversight mechanism makes personal data privacy vulnerable to abuse by authorities (Harsono, 2017).

The absence of clear standards regarding data security is another weakness of the existing legal framework. The ITE Law does not stipulate specific standards or data security requirements that must be met by data managers. This means that each entity may have different security standards, which can lead to inconsistencies in data protection and increase the risk of data leakage (Putri, 2019).

Furthermore, the sanctions imposed by the ITE Law on violations related to personal data are not sufficient to provide a deterrent effect. The existing sanctions focus more on the criminal aspect with imprisonment and fines, but do not provide restorative solutions that can repair the losses experienced by victims of personal data violations. This often makes victims of personal data violations feel that they are not getting adequate justice (Nugroho, 2020).

Facing the rapid dynamics of technology and frequent data leak incidents, it is clear that the ITE Law needs substantial updates to improve personal data protection. Legal reforms need to be carried out immediately to address these weaknesses, by adopting a more adaptive approach to technology and strengthening the right to personal data privacy.

In addition to the aforementioned issues, the legal framework for personal data protection in Indonesia also suffers from weaknesses in the absence of an independent and specific supervisory authority responsible for overseeing the implementation of personal data protection. In many countries, the establishment of such supervisory authorities has become a common practice to ensure compliance with data protection laws and to provide a venue for the public to file complaints about personal data violations (Anderson, 2019). In the Indonesian context, although the ITE Law provides several provisions on data protection, there is no specific body mandated to oversee data processing practices by private and government entities, which often results in a lack of effective enforcement.

In addition, the ITE Law also does not provide clear guidelines regarding data owner consent. Article 26 paragraph (1) states that anyone who uses electronic data containing personal data that is opened for public interest is required to obtain consent from the owner of the relevant personal data. However, this provision does not explain how the consent process must be carried out, what type of consent is sufficient (whether it must be written, electronic, or verbal), and how consent can be revoked by the data owner (Wibowo, 2021).

In the international aspect, Indonesia has also not ratified international conventions or agreements related to personal data protection, such as the Council of Europe Convention 108 on the Protection of Individuals against Automatic Processing of Personal Data. The absence of participation in the

international agreement shows Indonesia's lack of commitment and isolation in the discussion and implementation of global standards for personal data protection, which can have an impact on international trust and cooperation in the digital economy (Maulani, 2018).

From a technical perspective, the ITE Law does not include adequate provisions regarding data security and storage. In the era of big data and cloud computing, data security is very important. Inadequate regulations regarding data security allow for large-scale data leaks and misuse, which not only impact individuals but also national security (Jones, 2020).

Given these weaknesses, there are several recommendations for updating personal data protection laws in Indonesia:

1. Clear and Comprehensive Definition: Expanding the definition of personal data in the ITE Law or in new regulations specifically on personal data protection to include all types of data that can be used to identify an individual, either directly or indirectly.
2. Establishment of a Personal Data Supervisory Authority: Establishment of an independent body tasked with overseeing the processing of personal data, receiving complaints, and conducting investigations into data breaches.
3. Setting Clear Consent Standards: Establish detailed guidelines on the consent process, including the format, procedures, and how to withdraw consent that data managers must follow.
4. Ratification of International Conventions: Indonesia should consider ratifying the Council of Europe Convention 108 as well as other international conventions on personal data protection to ensure standards consistent with global practices.

Enhancing the Legal Framework for Personal Data Protection in Indonesia in the Context of Globalization

In an era of increasing globalization and digital interconnection, personal data protection has become a crucial issue for countries around the world, including Indonesia. To ensure effective personal data protection, Indonesia needs to improve its legal framework by adopting regulations and policies that are in line with international best practices and adapt them to the unique socio-economic context in Indonesia.

One of the first steps in improving personal data protection is to adopt international standards that have proven effective in regulating data protection. For example, the European Union's General Data Protection Regulation (GDPR) has become a model for many countries due to its stringent protection of personal data and clear provisions on data subject rights (EU, 2016). Indonesia can take inspiration from the GDPR to draft a comprehensive personal data protection law, which not only regulates the collection and use of personal data but also provides clear rights for individuals to control their data, including the right to be forgotten, the right to access data, and the right to rectify incorrect data (Thompson, 2018).

To ensure effective law enforcement, it is important for Indonesia to establish an independent supervisory authority that has the authority to supervise, sanction, and regulate sectors that collect and process personal data. This authority should have the power to conduct inspections and audits, as well as the authority to issue fines for violations of data protection laws. This model has proven successful in countries such as Ireland and Germany, where data protection authorities have an active role in maintaining compliance with data protection regulations (Bennett, 2019).

Raising awareness and education about the importance of personal data protection is another key aspect. The Indonesian government needs to invest resources in public education campaigns to raise

public awareness about their rights and corporate responsibilities in managing personal data. This also includes training for government officials and employees in the private sector on the importance of data security and good data governance (Suryadi, 2020).

Any policy implemented must take into account Indonesia's social and economic context. This includes recognizing the limitations of digital infrastructure in some areas, which may affect the implementation of data protection policies. Policies must be flexible to adapt to the needs of different sectors and scalable to encourage innovation while protecting personal data (Nakamura, 2021).

Indonesia should also actively participate in international forums and initiatives related to personal data protection to ensure that domestic regulations are in line with global trends and best practices. This cooperation could include exchanging information on cyber threats, handling cross-border data breaches, and harmonizing data protection standards (Lee, 2019).

One important aspect in improving the legal framework for personal data protection is the integration of technology in policy development. Technologies such as encryption and blockchain can provide more secure solutions for the management and storage of personal data. The Indonesian government can work with technology experts to develop adequate standards in the use of these technologies in data management, which not only improves data security but also efficiency in its management (Patel, 2020). This approach is in line with the principle of "Privacy by Design" which emphasizes that policies and technologies must be designed to protect user privacy from the beginning of system design to its execution.

Improving personal data protection requires cross-sector collaboration involving the government, private sector, and civil society. The government should take the initiative to establish a special forum or committee that focuses on the issue of personal data protection, involving all stakeholders. Through this forum, discussions and exchange of ideas can be held to strengthen regulations and practices for managing personal data in Indonesia. This collaborative approach will help in identifying specific needs and creating sustainable and inclusive solutions (Gomez, 2021).

In line with rapid technological developments, legal reforms must also be dynamic and responsive to these changes. Indonesia can consider adopting an adaptive legal model that allows for periodic revision and adjustment of the personal data protection law. This model allows the law to remain relevant and effective amidst ever-changing technology and evolving business practices. This can also include the implementation of sunset clauses in the law, where the law must be reviewed and updated periodically to ensure that the regulation remains relevant and effective (Harper, 2022).

Digital education and literacy are important foundations in improving personal data protection. The Indonesian government must launch a massive education initiative to raise public awareness about the importance of personal data protection. These programs must target all levels of society and involve various media, from workshops, seminars, online campaigns, to lessons in schools. Improving digital literacy will strengthen individuals' capacity to protect their own data and make informed decisions in their digital interactions (Martinez, 2021).

The development of infrastructure that supports data security is key to protecting personal data. The government must ensure that information technology infrastructure in Indonesia has strong security protection and complies with international standards. This includes data centers equipped with the latest technology for data security and data recovery mechanisms. The government must also encourage and support the private sector to implement high security standards in their operations (Johnson, 2020).

Strong and effective law enforcement is an essential element of the legal framework for personal data protection. Supervisory authorities should be given sufficient resources and broad powers to

conduct oversight, investigation and prosecution of personal data breaches. This includes the ability to impose severe sanctions for serious violations to provide a deterrent effect. Effective law enforcement will build public trust in the personal data protection system in Indonesia (White, 2019).

CONCLUSION

Legal protection of personal data in the digital era is an important issue that requires serious attention from all parties in Indonesia. Amidst the increasing pace of globalization and digitalization, a robust legal framework is needed to protect the privacy and security of citizens' personal data. The conclusions of this analysis point to several key aspects that must be strengthened to achieve effective data protection in Indonesia:

1. Adoption of International Standards: Indonesia should integrate international standards such as GDPR into its national legal framework to enhance personal data protection. These models offer a proven framework for regulating and protecting personal data that can be adapted to local contexts.
2. Establishment of an Independent Supervisory Authority: The establishment of an independent and strong supervisory authority is essential to oversee the implementation of data protection laws, ensure compliance by entities managing data, and provide confidence to the public that their rights are protected.
3. Public Education and Digital Literacy Enhancement: Initiatives to increase awareness and digital literacy should be expanded so that every individual can understand their rights regarding personal data and how to protect themselves in the digital environment.
4. Dynamic Legal Reform: The legal framework must be flexible and dynamic, able to adapt to rapid technological developments. This includes periodic reviews of existing laws and the implementation of regulations that are responsive to technological changes and new challenges.
5. Cross-Sector Collaboration: Collaboration between government, industry, and civil society needs to be enhanced to develop and implement effective policies on personal data protection. This collaborative approach will ensure that policies serve the interests of all parties and improve overall data protection standards.
6. Building Secure Infrastructure: Investment in secure technology infrastructure is crucial to ensuring the security of personal data. Governments and the private sector must collaborate to build and maintain infrastructure that can protect data from cyber threats and information leaks.

Through these steps, Indonesia will not only strengthen personal data protection but also position itself as a country that prioritizes human rights and security in the digital realm. This is important not only to protect individuals but also to support inclusive and sustainable digital economic growth.

BIBLIOGRAPHY

Anderson, K. (2019). Global Data Privacy: The EU Way. London: Springer.

Bennett, C. J. (2019). Regulatory Models for Data Protection: The Future of Privacy. Cambridge University Press.

EU (2016). General Data Protection Regulation (GDPR). Regulation (EU) 2016/679.

Gomez, E. (2021). Collaborative Approaches to Data Privacy. New York: Springer.

Harper, J. (2022). Adaptive Legal Frameworks for Data Protection. London: Routledge.

Harsono, A. (2017). The Dilemma of Privacy in Indonesia. Jakarta: University of Indonesia Press.

Johnson, R. (2020). "Building Secure Data Infrastructures: Challenges and Solutions," Journal of Cybersecurity, vol. 6, no. 1.

Jones, S. (2020). Security Protocols for Information Technology. Cambridge: Cambridge University Press.

Lee, H. (2019). "Global Trends in Privacy Regulation: Can ASEAN Lead the Way?" ASEAN Journal of Legal Studies, vol. 2, no. 1.

Martinez, L. (2021). Digital Literacy and Data Protection. San Francisco: Academic Press.

Maulani, C. (2018). "Indonesia's Isolation in International Data Protection Frameworks," Journal of Digital Law and Policy, vol. 4, no. 1, pp. 20-35.

Nakamura, R. (2021). "Adapting Data Protection Strategies to Emerging Markets: A Case Study of Indonesia", Journal of Information Policy, vol. 11.

Nugroho, L. (2020). Data Privacy and Security in Indonesia: Challenges and Solutions. Bandung: ITB Publisher.

Patel, S. (2020). "Innovative Technologies for Data Protection: The Role of Encryption and Blockchain," Technology Law Journal, vol. 15, no. 2.

Putri, TA (2019). Regulation and Protection of Personal Data in Indonesia. Yogyakarta: Gadjah Mada University Press.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Satrio, J. (2018). Personal Data Protection in Indonesian Law. Jakarta: Kencana.

Smith, J. (2020). Data Privacy Regulations in a Digital Age. Oxford University Press.

Suryadi, K. (2020). "Challenges and Opportunities in Implementing Data Protection Laws in Indonesia", Indonesian Law Review, vol. 20, no. 2.

Thompson, H. (2018). Data Privacy: Europe's GDPR and Its Global Effect. Informa UK Limited.

Law Number 11 of 2008 concerning Electronic Information and Transactions.

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.

White, C. (2019). "Effective Law Enforcement in Data Protection: A Critical Analysis," Legal Studies Review, vol. 39, no. 4.

Wibowo, A. (2021). Consent and Data Privacy in Indonesia. Yogyakarta: Gadjah Mada University Press.