

# Law for Ensuring Data Security in the Digital Age: Challenges for Government and Warnings for Us

Ariskita Duha<sup>1\*</sup>

Faculty of Law, Sari Mutiara University, Medan City, North Sumatra 20123, Indonesia

Email: [kitaaris\\_duha@gmail.com](mailto:kitaaris_duha@gmail.com)

ARTICLE INFO	ABSTRACT
Received: 25 Mar 2024	The rapid development of information technology in the digital era poses serious challenges to personal data protection. Data leakage, misuse of information, and unauthorized surveillance are real threats that require a comprehensive legal response. This study aims to analyze the extent of the role of law in ensuring data security in Indonesia, as well as evaluate the effectiveness of Law Number 27 of 2022 concerning Personal Data Protection. This study uses a normative juridical approach with a literature study method and comparative analysis of the General Data Protection Regulation (GDPR) as a reference for international standards. The results of the study show that even though Indonesia already has a formal legal basis through the PDP Law, the implementation of data protection still faces various obstacles. Among them are the lack of independent, authoritative institutions, the lack of public literacy related to digital privacy, and weak law enforcement against data breaches. A comparative study with GDPR confirms that Indonesia's legal framework is not yet equal in terms of transparency, accountability, and oversight of data controllers. The conclusion of this study shows that structural and substantial efforts are needed to strengthen the data protection legal system, including the drafting of technical regulations, institutional strengthening, and increasing the capacity of law enforcement human resources. The implications of this study emphasize the importance of regulatory reform and a multidisciplinary approach between law and technology to create an effective and equitable data protection system.
Accepted: 11 Jun 2024	
Published: 02 Aug 2024	
<b>Keywords:</b>	
Personal data protection, Data security, Privacy rights, Digital age, Data leaks	
<b>Doi:</b> <a href="https://doi.org/10.59011/vjlaws.3.2.2024.111-119">https://doi.org/10.59011/vjlaws.3.2.2024.111-119</a>	

## 1. Introduction

The development of information and communication technology has created a huge leap in digital transformation in almost all aspects of life.<sup>2</sup> In this context, data becomes

\* Corresponding Author

E-mail address: [kitaaris\\_duha@gmail.com](mailto:kitaaris_duha@gmail.com)

Copyright © 2024 The Author(s)

CC BY-NC 4.0 License

<sup>2</sup> Jinguang Guo and Hanqi Zhang, "Digital Age: The Path Choice of Government-Citizen Value Co-Creation," *Heliyon* 10, no. 15 (2024): e35482, <https://doi.org/10.1016/j.heliyon.2024.e35482>.

a very vital asset, not only for individuals but also for public and private institutions.<sup>3</sup> In today's digital age, personal data can be collected, stored, and processed on a large scale quickly and cheaply through technologies such as cloud computing, big data, and artificial intelligence.<sup>4</sup> However, these advances also bring new threats to data privacy and security. When personal data falls into the wrong hands, this can cause enormous legal and economic losses for data owners.<sup>5</sup>

Data security in the legal context has become a major concern in recent years, especially with the rise of data leaks, cyber hacks, and misuse of personal information. Personal data is no longer static, but can be analyzed to create individual profiles, influence political decisions, and shape people's consumptive behavior. As stated by Küzeci (2022), the absence of strong legal oversight of data processing leads to the emergence of practices that are detrimental and degrade to human dignity.<sup>6</sup>

Countries around the world are responding to this challenge by establishing various regulations to ensure data security and confidentiality. The European Union through the General Data Protection Regulation (GDPR)<sup>7</sup> has become a global reference in personal data protection regulations. These regulations provide strong rights for data subjects, including the right to be forgotten and the right to data portability. Countries such as Brazil, Japan, and even Indonesia have begun to adapt their regulations to the GDPR standard in an effort to strengthen the legal position of data subjects.<sup>8</sup>

However, law enforcement in the context of data protection is not always effective. One of the main challenges is the unpreparedness of law enforcement institutions in responding to the complexity of digital technology. In Indonesia, for example, even though Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)<sup>9</sup> has been passed, various cases of data leaks such as BPJS Kesehatan, MyIndiHome, and eHAC data leak incidents show weak implementation and enforcement of these regulations.<sup>10</sup>

In addition to institutional issues, there are also juridical challenges in the form of inconsistencies between national regulations and international norms. This causes legal disharmony that has the potential to create legal uncertainty in resolving cross-border data disputes.<sup>11</sup> In the context of globalization and cross-border data movements, legal

---

<sup>3</sup> Vera Zinovieva, Mikhail Shchelokov, and Evgeny Litvinovsky, "Legal Issues of Protection of Personal Data: Cases of Transport Data Leaks," *Transportation Research Procedia* 68 (2023): 461–67, <https://doi.org/10.1016/j.trpro.2023.02.062>.

<sup>4</sup> Fleur Johns, "Data, Detection, and the Redistribution of the Sensible in International Law," *American Journal of International Law* 111, no. 1 (2017): 57–103, <https://doi.org/10.1017/ajil.2016.4>.

<sup>5</sup> Mattias Holzhausen, "Legal Accountability and Ethical Considerations for Outcomes Driven by Artificial Intelligence in Business Operations," *Udayana Journal of Law and Culture* 8, no. 1 (2024): 1–23, <https://doi.org/10.24843/UJLC.2024.v08.i01.p01>.

<sup>6</sup> Elif Küzeci, "Personal Data Protection Law," *Introduction to Turkish Business Law*, no. 016999 (2022): 457–83.

<sup>7</sup> EU, *General Data Protection Regulation, Official Journal of the European Union*, 2016.

<sup>8</sup> Erna Priliyasi, "Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 12, no. 2 (2023): 261–79.

<sup>9</sup> Indonesian's Law, "Law Number 27 of 2022 Concerning Personal Data Protection in Indonesia" (2022).

<sup>10</sup> Naylawati Bahtiar, "Darurat Kebocoran Data: Kebutuhan Regulasi Pemerintah," *Development Policy and Management Review (DPMR)* 2, no. 1 (2022): 85–100.

<sup>11</sup> Aris Sarjito, "Data Security and Privacy in the Digital Era: Challenges for Modern Government," *JIAN (Jurnal Ilmiah Administrasi Negara)* 8, no. 3 (2024): 1–13, <https://doi.org/10.56071/jian.v8i3.933>.

integration between jurisdictions is indispensable to create comprehensive and universal data protection.<sup>12</sup>

This research departs from the urgency of the need to strengthen the role of law in ensuring data security in the midst of the onslaught of digitalization. The purpose of this study is to analyze the extent to which existing legal instruments are able to answer data security challenges in the digital era and provide relevant legal reform directions. This study also examines the effectiveness of normative juridical approaches in examining data protection, especially with a focus on the substance of regulations and their law enforcement systems. Thus, it is hoped that the results of this research can contribute to the formulation of policies that favor people's digital rights.

## 2. Legal Methods and Materials

This research uses the normative juridical method, which is an approach that relies on the analysis of positive legal norms, both written in laws and regulations and those contained in general law principles<sup>13</sup>. This approach is used to understand how national and international legal systems respond to personal data security issues in the context of the digital age. This approach is relevant because the issue of data protection is a normative issue that is closely related to the principles of legality, human rights, and the rule of law.

In order to obtain a comprehensive overview of the role of law in ensuring data security, the legal materials used in this study are divided into two types: (1) primary legal material, namely laws and regulations directly related to the protection and security of personal data. These materials include:

- Law Number 27 of 2022 concerning Personal Data Protection (PDP Law);
- Law Number 11 of 2008 concerning Information and Electronic Transactions and its amendments (ITE Law);
- Government Regulations, Ministerial Regulations, and Regulations of relevant Authorities (e.g. Kominfo, BSSN);
- General Data Protection Regulation (GDPR) from the European Union as a global data protection standard;
- Brazil's LGPD and Japan's APPI regulations as legal comparisons.

Then, (2) secondary legal materials, namely scientific literature such as books, legal journals, results of scientific seminars, and research reports that discuss legal aspects of personal data protections.

The analysis technique used is qualitative analysis, by interpreting the applicable legal norms and comparing them with factual practices or implementations in the field, including cases of data leaks that have occurred in Indonesia. This analysis is then combined with a comparative law approach to data protection systems from other more

---

<sup>12</sup> Daniel J Solove, *The New Vulnerability: Data Security and Personal Information*, ed. Radin and Chander (Stanford: Stanford University Press, 2008).

<sup>13</sup> Peter Mahmud Marzuki, *Penelitian Hukum*, Cet. XIV (Jakarta: Prenada Media Group, 2019).

advanced countries, such as the European Union and Japan, to assess the strengths and weaknesses of Indonesia's legal system.

### 3. Results and Discussion

The digital age has brought about a major transformation in people's lives, including in the way personal data is collected, stored, and used. In the midst of the surge in the use of information technology, concerns have arisen about data security and privacy, especially with the rampant cases of data leaks in Indonesia.<sup>14</sup> Therefore, data protection regulations are an important instrument that not only guarantees citizens' right to privacy, but also becomes the foundation for building public trust in the implementation of digital systems. The following discussion will outline the main findings of this study based on a normative juridical approach that examines the positive legal framework, enforcement effectiveness, and its comparison with international practice.

#### 1. Ineffective Regulation and Weak Implementation of the PDP Law in Indonesia

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is an initial milestone for Indonesia in providing a legal framework to ensure the security of personal data. However, until now, the implementation of the law is still far from optimal. One of the main obstacles lies in the slow establishment of independent supervisory bodies that are supposed to function as data protection authorities. Without this institution, the PDP Law tends to be symbolic and does not have adequate enforcement power.<sup>15</sup> In addition, in practice, the mechanism for complaints, investigations, and sanctions against data breaches is still unstructured. This has caused many cases of data leaks such as BPJS Kesehatan, eHAC, and MyIndiHome not to receive adequate legal handling. The unclear role of technical institutions such as the Ministry of Communication and Information and BSSN in the context of supervision makes the PDP Law ineffective in providing real protection for individuals.

Another weakness lies in the lack of technical understanding of law enforcement officials on the substance of the PDP Law. Many investigators have not received special training on digital forensics and data management systems, making the evidentiary process in data breach cases difficult. This situation creates a legal gray space that can actually be exploited by data breach perpetrators.<sup>16</sup>

In fact, in a data protection system, effectiveness is not only determined by normative substance, but also by legal infrastructure and supporting technology. Without the readiness of human resources and information technology support, regulations will remain a weak normative statement in their implementation.

---

<sup>14</sup> Budi Prasetyo, I Gusti Ayu Ketut Rachmi Handayani, and Adi Sulistiyono, "Data Protection Laws in Indonesia: Navigating Privacy in the Digital Age," *SIDE: Scientific Development Journal* 2, no. 1 (2025): 9–16.

<sup>15</sup> Indonesian's Law, Law Number 27 of 2022 concerning Personal Data Protection in Indonesia.

<sup>16</sup> Rudi Natamiharja and Ikhsan Setiawan, "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France," *Jambe Law Journal* 7, no. 1 (2024): 233–51, <https://doi.org/10.22437/home.v7i1.349>.

## 2. Comparison with International Regulations: The Dominance of GDPR as a Global Standard

The European Union's General Data Protection Regulation (GDPR) has become a global standard in personal data protection. The GDPR offers a legal framework that is not only comprehensive but also responsive to technological developments. One of the advantages is the regulation of basic principles such as lawful basis, data minimization, and data subject rights that are clearly and operationally described. According to Pazhohan (2022), GDPR effectively forces multinational companies to conduct audits of their data systems to align with data protection principles.<sup>17</sup> Companies that fail to comply can be fined up to 4% of total global annual revenue, a sanction mechanism that Indonesia's PDP Law does not yet have.

Apart from the legal substance, GDPR is also supported by enforcement agencies such as the Data Protection Authority (DPA) in each member country that has clear authority. This is inversely proportional to the situation in Indonesia, where data supervisory institutions have not been formed functionally so that public complaints often do not receive a systematic response. International regulations such as GDPR not only provide legal protection for individuals, but also enhance a country's digital competitiveness. GDPR-compliant countries gain international trust in digital trade and cross-border data flows.<sup>18</sup>

## 3. Law Enforcement Challenges: Absence of Effective Criminal Sanctions

The law enforcement aspect is a crucial challenge in ensuring data security.<sup>19</sup> Although the PDP Law contains criminal provisions, its implementation in the field is very limited. This is due to the unpreparedness of the law enforcement and the lack of technical guidelines in the implementation of sanction articles. The effectiveness of law enforcement depends on legal certainty and consistency of implementation.<sup>20</sup> In Indonesia, weak coordination between technical institutions such as BSSN, the Ministry of Communication and Information, and the police hinders the investigation process of data leak cases. Without clear SOPs, law enforcement is unable to process data breaches professionally and fairly.

On the other hand, there is no strong jurisprudence in data breach cases<sup>21</sup>, so judges and prosecutors are still hesitant to apply sanctions based on the PDP Law.

---

<sup>17</sup> Helia Pazhohan, "Global Data Protection Standards: A Comparative Analysis of GDPR and Other International Privacy Laws," *Legal Studies in Digital Age* 2, no. 3 (2023): 1–12.

<sup>18</sup> Syed Khurram Hussain Naqvi and Komal Batool, "A Comparative Analysis between General Data Protection Regulations and California Consumer Privacy Act," *Journal of Computer Science, Information Technology and Telecommunication Engineering* 4, no. 1 (2023): 326–32, <https://doi.org/10.30596/jcositte.v4i1.13330>.

<sup>19</sup> Sekaring Ayumeida Kusnadi, "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi," *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16, <https://doi.org/10.47776/alwasath.v2i1.127>.

<sup>20</sup> Li Adik Aleksandrovich, "Cyber Law: Addressing Legal Challenges in the Digital Age," *Uzbek Journal of Law and Digital Policy* 1, no. 3 (2023): 1–11, <https://doi.org/10.59022/ujldp.92>.

<sup>21</sup> Spencer Wheatley, Thomas Maillart, and Didier Sornette, "The Extreme Risk of Personal Data Breaches and the Erosion of Privacy," *The European Physical Journal B* 89, no. 1 (2016): 7, <https://doi.org/10.1140/epjb/e2015-60754-4>.

This indicates an urgent need for digital legal training for law enforcement and the integration of electronic systems that facilitate digital forensic reporting and proof.<sup>22</sup> Not optimal law enforcement also sends a negative message to the public and business actors that violations of personal data are not serious violations. In fact, losses due to data breaches can include identity misuse, digital fraud, and even economic exploitation.

#### **4. Inequality of Legal Literacy and Data Protection Awareness**

Data security problems do not only come from regulatory aspects, but also from low legal literacy and public awareness about their rights to personal data. Many individuals are unaware that their data is collected, processed, and even sold by digital service providers without explicit consent. Digital privacy literacy is a key element in strengthening the implementation of data protection regulations.<sup>23</sup> Without adequate public understanding, the rights guaranteed by the law cannot be enforced because the public does not know how to protect or demand those rights.

Public campaigns by the government and civil society organizations are still minimal. Digital education programs still focus on the use of technology, not on the ethical and legal aspects of data use.<sup>24</sup> As a result, society becomes passive and permissive towards privacy violations. This situation is exacerbated by the lack of transparency from digital business actors in explaining privacy policies. Many users do not read or understand the terms and conditions of use of data, which are often technical and complex. This requires regulations that require platform providers to convey privacy information in a simple and easy-to-understand manner.

#### **5. The Need for Regulatory Harmonization and Institutional Capacity Building**

To realize a comprehensive data protection system, it is necessary to harmonize the PDP Law with other sector regulations such as the ITE Law, financial regulations, and BSSN regulations. In addition, strengthening institutional capacity through training and certification of digital legal employees is urgently needed. The importance of aligning public policies between state institutions to prevent regulatory overlap and create legal certainty for business actors and the public.<sup>25</sup>

#### **4. Conclusion**

This research shows that the role of law in ensuring data security in the digital era has not been running optimally, especially in the Indonesian context. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) has become an important milestone

---

<sup>22</sup> Lena Klasén, Niclas Fock, and Robert Forchheimer, "The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age," *Forensic Science International* 362 (2024): 112133, <https://doi.org/10.1016/j.forsciint.2024.112133>.

<sup>23</sup> Muhammad Fadly Nasution, "The Role of Civil Law in the Protection of Privacy and Personal Data," *Innovative: Journal Of Social Science Research* 3, no. 2 (2023): 3669–79.

<sup>24</sup> Nasution.

<sup>25</sup> Joshua Filani, "Data Privacy in the Digital Age: Analyzing the Impact of Technology of U.S Privacy Regulations," *SSRN Electronic Journal* 1, no. 217 (2024): 1–19, <https://doi.org/10.2139/ssrn.4762809>.

in forming a legal framework that regulates personal data protection. However, the effectiveness of its implementation is still constrained by weak supervision institutions, limited law enforcement resources, and the lack of derivative regulations that comprehensively regulate technical procedures for data protection.

A comparison with GDPR as an international data protection standard shows that Indonesia's legal system still has many weaknesses, especially in terms of sanctions enforcement, protection of data subject rights, and the capacity of supervisory institutions. In addition, other challenges include low public literacy related to digital privacy and lack of public participation in overseeing data protection policies. The implications of these findings include several aspects. First, relatively, it is necessary to accelerate the establishment of an independent data protection authority institution with clear authority to carry out the mandate of the PDP Law. Second, there is a need for harmonization of technical regulations that can describe the principles of data protection practically, especially in the public service and digital business sectors. Third, the government needs to initiate a massive legal and digital literacy program so that people are able to understand their rights and play an active role in maintaining data privacy. Fourth, training law enforcement officials and establishing standard operating procedures for handling data breaches are urgent needs to ensure legal certainty and justice.

### **Conflict of interest**

The author declares that there is no conflict of interest in making this article.

### **Authors' contribution**

The author state that author made substantial contributions to the conception and design of the study. The author took responsibility for data analysis, interpretation and discussion of results with the assistance of OpenAI. The author reads and approved the final manuscript.

### **References**

- Aleksandrovich, Li Adik. "Cyber Law: Addressing Legal Challenges in the Digital Age." *Uzbek Journal of Law and Digital Policy* 1, no. 3 (2023): 1–11. <https://doi.org/10.59022/ujldp.92>.
- Bahtiar, Naylawati. "Darurat Kebocoran Data: Kebutuhan Regulasi Pemerintah." *Development Policy and Management Review (DPMR)* 2, no. 1 (2022): 85–100.
- EU. *General Data Protection Regulation. Official Journal of the European Union*, 2016.
- Filani, Joshua. "Data Privacy in the Digital Age: Analyzing the Impact of Technology of U.S Privacy Regulations." *SSRN Electronic Journal* 1, no. 217 (2024): 1–19. <https://doi.org/10.2139/ssrn.4762809>.
- Guo, Jinguang, and Hanqi Zhang. "Digital Age: The Path Choice of Government-Citizen Value Co-Creation." *Heliyon* 10, no. 15 (2024): e35482. <https://doi.org/10.1016/j.heliyon.2024.e35482>.

- Holzhausen, Mattias. "Legal Accountability and Ethical Considerations for Outcomes Driven by Artificial Intelligence in Business Operations." *Udayana Journal of Law and Culture* 8, no. 1 (2024): 1–23. <https://doi.org/10.24843/UJLC.2024.v08.i01.p01>.
- Indonesian's Law. Law Number 27 of 2022 concerning Personal Data Protection in Indonesia (2022).
- Johns, Fleur. "Data, Detection, and the Redistribution of the Sensible in International Law." *American Journal of International Law* 111, no. 1 (2017): 57–103. <https://doi.org/10.1017/ajil.2016.4>.
- Klasén, Lena, Niclas Fock, and Robert Forchheimer. "The Invisible Evidence: Digital Forensics as Key to Solving Crimes in the Digital Age." *Forensic Science International* 362 (2024): 112133. <https://doi.org/10.1016/j.forsciint.2024.112133>.
- Kusnadi, Sekaring Ayumeida. "Perlindungan Hukum Data Pribadi Sebagai Hak Privasi." *AL WASATH Jurnal Ilmu Hukum* 2, no. 1 (2021): 9–16. <https://doi.org/10.47776/alwasath.v2i1.127>.
- Küzeci, Elif. "Personal Data Protection Law." *Introduction to Turkish Business Law*, no. 016999 (2022): 457–83.
- Marzuki, Peter Mahmud. *Penelitian Hukum*. Cet. XIV. Jakarta: Prenada Media Group, 2019.
- Naqvi, Syed Khurram Hussain, and Komal Batool. "A Comparative Analysis between General Data Protection Regulations and California Consumer Privacy Act." *Journal of Computer Science, Information Technology and Telecommunication Engineering* 4, no. 1 (2023): 326–32. <https://doi.org/10.30596/jcositte.v4i1.13330>.
- Nasution, Muhammad Fadly. "The Role of Civil Law in the Protection of Privacy and Personal Data." *Innovative: Journal Of Social Science Research* 3, no. 2 (2023): 3669–79.
- Natamiharja, Rudi, and Ikhsan Setiawan. "Guarding Privacy in the Digital Age: A Comparative Analysis of Data Protection Strategies in Indonesia and France." *Jambe Law Journal* 7, no. 1 (2024): 233–51. <https://doi.org/10.22437/home.v7i1.349>.
- Pazhohan, Helia. "Global Data Protection Standards: A Comparative Analysis of GDPR and Other International Privacy Laws." *Legal Studies in Digital Age* 2, no. 3 (2023): 1–12.
- Prasetyo, Budi, I Gusti Ayu Ketut Rachmi Handayani, and Adi Sulistiyono. "Data Protection Laws in Indonesia: Navigating Privacy in the Digital Age." *SIDE: Scientifict Development Journal* 2, no. 1 (2025): 9–16.
- Priliasari, Erna. "Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce Menurut Peraturan Perundang-Undangan Di Indonesia." *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 12, no. 2 (2023): 261–79.
- Sarjito, Aris. "Data Security and Privacy in the Digital Era: Challenges for Modern Government." *JIAN (Jurnal Ilmiah Administrasi Negara)* 8, no. 3 (2024): 1–13. <https://doi.org/10.56071/jian.v8i3.933>.
- Solove, Daniel J. *The New Vulnerability: Data Security and Personal Information*. Edited



- by Radin and Chander. Stanford: Stanford University Press, 2008.
- Wheatley, Spencer, Thomas Maillart, and Didier Sornette. “The Extreme Risk of Personal Data Breaches and the Erosion of Privacy.” *The European Physical Journal B* 89, no. 1 (2016): 7. <https://doi.org/10.1140/epjb/e2015-60754-4>.
- Zinovieva, Vera, Mikhail Shchelokov, and Evgeny Litvinovsky. “Legal Issues of Protection of Personal Data: Cases of Transport Data Leaks.” *Transportation Research Procedia* 68 (2023): 461–67. <https://doi.org/10.1016/j.trpro.2023.02.062>.