PT. Lentera Ilmu Publisher

Online version at https://journal.lenterailmu.com/index.php/josapen

JOSAPEN

JOURNAL OF COMPUTER SCIENCE APPLICATION AND ENGINEERING

E-ISSN: 3031-2272 (Online)

Ensuring Data Privacy in the Age of Artificial Intelligence

Yatama Zahra

Faculty of Law, Sriwijaya University, Palembang, Indonesia

ARTICLE INFO

Article history:
Received 30 June 2025
Revised 01 Aug 2025
Accepted 01 Aug 2025

Keywords:
Artificial Intelligence
Data Privacy
Personal Data Protection Law

ABSTRACT

This study explores the intersection of data privacy and artificial intelligence (AI) within the context of Indonesia's evolving digital landscape. As AI technologies become increasingly embedded in key sectors such as healthcare, finance, education, and public services, the need for robust data protection mechanisms grows more urgent. The 2022 enactment of Indonesia's Personal Data Protection (PDP) Law marks a significant step toward safeguarding individual privacy rights and regulating the use of personal data in AI systems. However, challenges remain in ensuring compliance with legal principles such as transparency, purpose limitation, and user consent, especially as many AI models operate as opaque "black boxes." Through a comparative analysis of global data privacy regulations—including the GDPR, CCPA, and PIPL—this study highlights international best practices and their relevance to AI governance. A conceptual framework is presented to illustrate the foundational principles necessary for aligning AI development with data privacy standards. The study concludes by emphasizing the importance of a harmonized, ethics-driven regulatory approach that supports responsible AI innovation while protecting individual rights. Stronger collaboration among government, industry, and civil society is essential to achieving a secure, trustworthy, and inclusive digital future for Indonesia.

1. Introduction

Artificial intelligence (AI) has rapidly become an integral part of digital transformation journey, powering innovations in sectors such as finance, education, health, and public services [1]-[3]. At the heart of many AI systems lies the collection and processing of personal data, which, if not properly managed, can pose serious risks to privacy and individual rights. The benefits of AI—such as improved efficiency, personalized services, and data-driven decision-making—must be weighed against the potential for misuse, especially in a landscape where data governance is still maturing. In response to these growing concerns, Indonesia enacted the Personal Data Protection (PDP) Law in 2022, marking a significant milestone in the country's effort to strengthen digital rights and data privacy. The PDP Law aims to provide legal clarity around the collection, processing, and protection of personal data, including data used by AI systems. However, despite this progress, challenges remain in ensuring that AI technologies comply with the principles outlined in the law,

* *Corresponding author:* Yatama Zahra
email: yatama@lenterailmu.com

such as transparency, purpose limitation, and accountability. Many AI systems operate as black boxes, making it difficult for individuals to know how their data is used or to exercise their rights under the law.

As AI applications become more embedded in daily life [4]-[8], the tension between technological innovation and data protection becomes more pronounced. For example, AI-based facial recognition in public spaces or algorithmic profiling in e-commerce raises important questions about informed consent, data minimization, and fairness. Enforcement mechanisms under the PDP Law are still developing, and there is a need for stronger collaboration between government agencies, technology companies, and civil society to ensure AI systems are both effective and legally compliant. Ensuring data privacy in the age of artificial intelligence is not only a matter of regulatory compliance—it is a critical foundation for public trust and responsible innovation. The successful implementation of the PDP Law must go hand in hand with education, ethical standards, and robust technological safeguards. As Indonesia continues to embrace digital transformation, protecting personal data in AI systems will be essential to achieving a just, secure, and inclusive digital future for all citizens.

2. Result and Discussion

In an increasingly digital world, the protection of personal data has become a critical concern for individuals, organizations, and governments alike. To address these concerns, various countries have enacted data privacy laws aimed at regulating how personal information is collected, processed, stored, and shared. These laws not only establish the rights of data subjects but also impose strict obligations on data controllers and processors to ensure transparency, accountability, and security. The table below presents a selection of prominent data privacy regulations from different regions, highlighting their scope, year of enactment, and key provisions. Table 1 shows the key data privacy regulations from various countries and regions, highlighting the year each law was enacted along with its core provisions.

Table 1 - The key data privacy regulations from various countries and regions

Regulation Name	Country/Region	Year Enacted	Key Provisions
General Data Protection Regulation (GDPR) [9]-[10]	European Union	2018	Protects personal data of EU citizens; governs consent, access rights, right to be forgotten, etc.
California Consumer Privacy Act (CCPA) [11]-[12]	USA (California)	2020	Grants consumers rights to access, delete, and opt-out of the sale of their personal data.
Personal Data Protection Act (PDPA)	Singapore	2012	Regulates collection, use, and disclosure of personal data by organizations.
Personal Information Protection Law (PIPL)	China	2021	Establishes data processing principles, cross-border data protections, and individual rights.
Data Privacy Act	Philippines	2012	Ensures the privacy of individuals' personal information and sets obligations for data controllers.
Protection of Personal Information Act (POPIA)	South Africa	2021	Covers data subject rights, explicit consent, and responsibilities of data processors and controllers.
Law No. 27 of 2022 on Personal Data Protection	Indonesia	2022	Governs personal data protection across public and private sectors, data subject rights, and criminal fines.

The table highlights how different countries have taken unique but converging approaches to personal data protection. The European Union's GDPR, for instance, is widely considered the global benchmark due to its comprehensive scope and strict enforcement mechanisms. It introduced principles such as explicit consent, the right to be forgotten, and data portability—ideas that have since influenced similar regulations worldwide. Likewise, the California Consumer Privacy Act (CCPA) represents a major step in U.S. state-level legislation, granting consumers the right to know, delete, and opt out of the sale of their personal data. These regulations emphasize user control and transparency, reflecting a growing demand for digital accountability in both public and private sectors.

Other countries have followed suit, tailoring data privacy laws to fit their socio-political contexts. Singapore's PDPA and the Philippines' Data Privacy Act, for example, provide structured guidelines for organizations to manage data responsibly, while China's PIPL takes a more state-centric approach, with strict provisions on cross-border data transfers and national security concerns. In Africa, South Africa's POPIA and Indonesia's Law No. 27 of 2022 signal a rising commitment to digital rights, placing greater emphasis on consent and enforcement. Together, these laws demonstrate a global trend: governments are increasingly prioritizing individuals' rights over their personal data, demanding higher standards of transparency and ethical responsibility from organizations in the digital age.

Data privacy regulations outlined in the table have direct and increasingly significant implications for artificial intelligence (AI), especially as AI systems rely heavily on large datasets—often containing personal or sensitive information. One of the foundational principles across laws like the GDPR, PIPL, and CCPA is the requirement for a lawful basis to process personal data. For AI, this means that any data used for model training, prediction, or profiling must be collected and processed with explicit consent or under clearly defined legal grounds. This poses a challenge for AI developers, particularly when dealing with legacy datasets or data collected without specific user awareness.

Transparency is another key area where privacy law intersects with AI [13]-[16]. Regulations such as the GDPR require that individuals be informed about how their data is used and, in the case of automated decision-making, be given an explanation of how decisions are made. This has led to a growing demand for explainable AI (XAI) models, which can provide understandable reasoning behind outcomes like loan approvals, job recommendations, or healthcare diagnostics. Similarly, laws restrict decisions made solely by algorithms if those decisions significantly affect individuals—giving them the right to human intervention and review.

Data minimization and purpose limitation principles also affect AI systems by requiring developers to only collect data necessary for a specific, stated purpose. This undermines the practice of indiscriminate data scraping or broad-purpose data aggregation for AI training. Additionally, global AI projects often involve transferring data across borders—something tightly regulated by laws like the GDPR and China’s PIPL. Organizations must ensure that such transfers meet international adequacy standards, which adds a layer of complexity when using cloud-based AI platforms hosted in different jurisdictions.

Finally, data privacy laws grant individuals the right to access, modify, delete, or restrict the use of their personal data—creating new technical challenges for AI developers. For instance, if a person requests deletion of their data, companies must be able to locate and remove that data even from trained models or derivative outputs. Some regulations also mandate conducting Data Protection Impact Assessments (DPIAs) before deploying AI systems that pose high risks to individual rights, such as facial recognition or automated profiling. This pushes organizations to adopt responsible AI practices, emphasizing ethics, accountability, and compliance as essential components of AI development.

The visual model on Figure 1 illustrates the core principles at the intersection of data privacy and AI regulation, focusing on four essential components: *lawful basis for processing*, *transparency*, *data minimization*, and *data subject rights*. At the center of the framework is a symbolic shield and padlock, representing the protective intent of these regulations. The arrows connecting each component emphasize that these principles are not isolated—they interact and reinforce one another. For example, a lawful basis for data processing cannot be meaningfully upheld without transparency, as users must understand how their data is used to give informed consent.

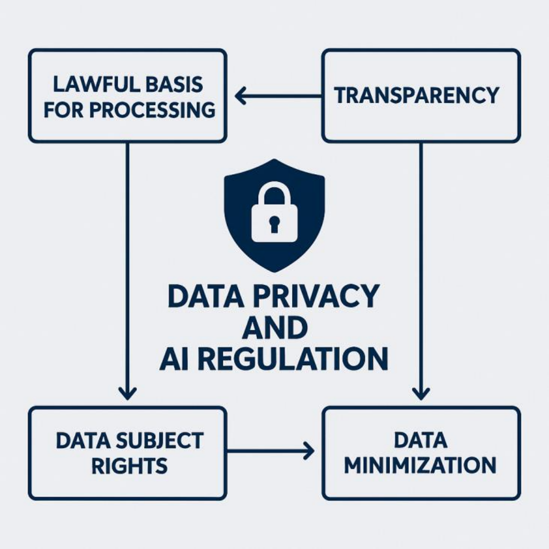

Figure 1 – Simple Framework for Data Privacy and AI Regulation

Starting from a lawful basis, organizations must justify the collection and use of personal data, especially when training or deploying AI systems. Transparency ensures that users are informed about automated processes, including profiling or algorithmic decisions. Data minimization limits the data collected to only what's necessary, discouraging large-scale harvesting without clear purpose. Finally, data subject rights give individuals control—allowing them to access, correct, or request deletion of their data. In an AI context, this framework guides ethical development, balancing innovation with individual rights and accountability.

To build a more trustworthy and future-ready landscape, data privacy and AI regulations must evolve toward a harmonized, proactive, and technology-informed framework. This includes developing globally aligned standards that address cross-border data flows while still respecting local values and rights. Regulators should also promote privacy-by-design and AI ethics-by-default principles—encouraging developers to integrate privacy, fairness, and transparency into algorithms from the earliest stages. Additionally, regulatory frameworks must become more agile, capable of adapting to rapid advances in AI, such as generative models and autonomous systems, while ensuring that individuals maintain meaningful control over their data. Stronger public-private collaboration, continuous policy review, and investment in explainable and auditable AI systems will be key to securing both innovation and human rights in the digital age.

4. Conclusion

The intersection of data privacy and artificial intelligence presents both an urgent challenge and a unique opportunity for Indonesia and the global community. While the enactment of Indonesia’s Personal Data Protection Law signifies a promising step forward, the effective governance of AI technologies will depend on more than legislation alone—it requires a cultural and institutional shift toward ethical data practices, transparency, and accountability. As AI becomes increasingly embedded in everyday services, maintaining public trust hinges on how well privacy protections are implemented and enforced. By embracing a balanced approach that supports innovation while safeguarding individual rights, Indonesia can build a more resilient, fair, and inclusive digital future—one where AI not only drives progress but also respects the dignity and autonomy of every citizen.

REFERENCES

[1] A. Bin Rashid and M. A. K. Kausik, “AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications,” *Hybrid Adv.*, vol. 7, no. July, p. 100277, 2024, doi: https://doi.org/10.1016/j.hybadv.2024.100277.

[2] F. Buonocore, M. C. Annosi, D. de Gennaro, and F. Riemma, “Digital transformation and social change: Leadership strategies for responsible innovation,” *J. Eng. Technol. Manag. - JET-M*, vol. 74, no. July, p. 101843, 2024, doi: https://doi.org/10.1016/j.jengtecman.2024.101843.

[3] V. Kumar, A. R. Ashraf, and W. Nadeem, “AI-powered marketing: What, where, and how?,” *Int. J. Inf. Manage.*, vol. 77, no. December 2023, p. 102783, 2024, doi: https://doi.org/10.1016/j.ijinfomgt.2024.102783.

[4] X. Yue, H. Li, and L. Meng, “AI-based Prevention Embedded System Against COVID-19 in Daily Life,” *Procedia Comput. Sci.*, vol. 202, pp. 152–157, 2022, doi: https://doi.org/10.1016/j.procs.2022.04.021.

[5] F. Hussain *et al.*, “A smartphone accelerometer data-driven approach to recognize activities of daily life: A comparative study,” *Smart Heal.*, vol. 30, no. July, p. 100432, 2023, doi: https://doi.org/10.1016/j.smhl.2023.100432.

[6] M. E. Ahmed, H. Yu, M. Vassallo, and P. Koufaki, “Advancing real-world applications: A scoping review on emerging wearable technologies for recognizing activities of daily living,” *Smart Heal.*, vol. 36, no. March, p. 100555, 2025, doi: https://doi.org/10.1016/j.smhl.2025.100555.

[7] M. Ghosh, “Decoding user readiness for sustainable AI adoption: A behavioural approach through technology readiness segmentation (TRS),” *Sustain. Futur.*, vol. 10, no. July, p. 100951, 2025, doi: https://doi.org/10.1016/j.sftr.2025.100951.

[8] M. Javaid, A. Haleem, S. Rab, R. Pratap Singh, and R. Suman, “Sensors for daily life: A review,” *Sensors Int.*, vol. 2, no. July, p. 100121, 2021, doi: https://doi.org/10.1016/j.sintl.2021.100121.

[9] K. M. Miller, K. Lukic, and B. Skiera, “The impact of the General Data Protection Regulation (GDPR) on online tracking,” *Int. J. Res. Mark.*, no. xxxx, 2025, doi: https://doi.org/10.1016/j.ijresmar.2025.03.002.

[10] D. A. Tamburri, “Design principles for the General Data Protection Regulation (GDPR): A formal concept analysis and its evaluation,” *Inf. Syst.*, vol. 91, p. 101469, 2020, doi: https://doi.org/10.1016/j.is.2019.101469.

[11] D. Bounie, A. Dubus, and P. Waelbroeck, “Collecting and Selling Consumer Information : Selling Mechanisms Matter ∗,” *Int. J. Ind. Organ.*, p. 103185, 2025, doi: https://doi.org/10.1016/j.ijindorg.2025.103185.

[12] O. Haggag, A. Pedace, S. Pan, and J. Grundy, “An analysis of privacy regulations and user concerns of finance mobile applications,” *Inf. Softw. Technol.*, vol. 184, no. April, p. 107756, 2025, doi: https://doi.org/10.1016/j.infsof.2025.107756.

[13] J. R. Saura, V. Škare, and D. O. Dosen, “Is AI-based digital marketing ethical? Assessing a new data privacy paradox,” *J. Innov. Knowl.*, vol. 9, no. 4, 2024, doi: https://doi.org/10.1016/j.jik.2024.100597.

[14] Z. Garroussi, A. Legrain, S. Gambs, V. Gautrais, and B. Sansò, “A systematic review of data privacy in Mobility as a Service (MaaS),” *Transp. Res. Interdiscip. Perspect.*, vol. 31, no. March 2024, 2025, doi: https://doi.org/10.1016/j.trip.2024.101254.

[15] M. Basha and G. Rodríguez-Pérez, “Trust, transparency, and adoption in generative AI for software engineering: Insights from Twitter discourse,” *Inf. Softw. Technol.*, vol. 186, no. September 2024, p. 107804, 2025, doi: https://doi.org/10.1016/j.infsof.2025.107804.

[16] C. Fontes, E. Hohma, C. C. Corrigan, and C. Lütge, “AI-powered public surveillance systems: why we (might) need them and how we want them,” *Technol. Soc.*, vol. 71, no. May, p. 102137, 2022, doi: https://doi.org/10.1016/j.techsoc.2022.102137.