Injurity: Interdiciplinary Journal and Humanity

Volume 4, Number 6, June 2025

e-ISSN: 2963-4113 and p-ISSN: 2963-3397

The Role of Artificial Intelligence in the Implementation of Personal Data Protection Law in Indonesia

Nina Purwanti[1], Megawati Barthos[2], Tri Eka Saputra[3]
[1,2]Universitas Borobudur, Indonesia,
[3]Universitas Mega Buana Palopo, Indonesia
Email: chimpaq13@gmail.com, megawati_barthos@borobudur.ac.id,
triekasaputra@gmail.com

Abstract

The development of artificial intelligence technology has brought significant impacts in various elements of daily life, such as in systems for managing personal data. Examining how artificial intelligence works in Indonesia's implementation of Law Number 27 of 2022 on the Protection of Personal Data is the aim of this study. The primary subjects of conversation are the legality of handling personal data with AI technology and the function of AI in Indonesia's execution of the Personal Data Protection Act. Normative legal research using a legislative framework is the methodology employed and analytical approach, through literature study of regulations, legal literature, and related policies. The results showed that: The role of artificial intelligence in the implementation of Law No. 27 of 2022 on Personal Data Protection in Indonesia presents both efficiency opportunities and serious challenges to the protection of individual privacy rights. Although this law has adopted data protection principles according to international standards, the unavailability of technical regulations and accountability mechanisms for the use of artificial intelligence creates a legal gap that needs to be addressed immediately. Therefore, legal certainty over the use of this technology requires regulations that are adaptive, principle-based, and uphold human rights through institutional strengthening, algorithmic supervision, and the application of the principle of explainability in responsive and humanist governance. This research recommends the need to strengthen technical regulations, algorithmic accountability mechanisms, and adaptive institutional supervision so that Human rights and legal certainty are upheld when artificial intelligence is used to manage personal data.

Keywords: Artificial Intelligence, Personal Data Protection, Digital Law

INTRODUCTION

The development of digital technology in the 21st century has changed the way humans live their daily lives. Amid rapid globalization and digitalization, artificial intelligence technology has become an important pillar in the transformation of various sectors, including law, education, health, finance, and public services. Artificial intelligence not only brings efficiency, automation, and data analysis at scale but also opens up new opportunities for more accurate and rapid decision-making. However, behind this progress, there are serious challenges concerning fundamental human rights, one of which is the protection of personal data.

Personal data is now a valuable commodity in the digital ecosystem. The activities of internet users recorded through search engines, social media applications, e-commerce, and digital-based government services generate a huge digital footprint. This data is then processed by artificial intelligence systems for various purposes, ranging from personally targeted advertisements, credit scoring, to predicting user behavior. In other words, the primary force behind the extensive and ongoing use of personal data is artificial intelligence. The dependence on artificial intelligence in managing data brings fundamental issues in the context of protecting privacy rights, controlling personal information, and technological accountability, which is often *"black box"* in nature.

Globally, various countries have recognized the necessity of protecting personal information by implementing stringent legal frameworks. For instance, the rights of data subjects and the obligations of data processors are governed by the General Data Protection Regulation (GDPR), a global data protection regulation, which was implemented by the European Union in 2018, along with responsibilities in the use of automation technologies, including artificial intelligence. The GDPR explicitly regulates the right to explanation for decisions that are entirely algorithm-generated, which is a response to the complexity and potential for discrimination in artificial intelligence systems. This marks a global legal awareness of the urgency of ensuring the principles of fairness, transparency, and accountability in a digital age driven by smart technology.

In the Asian region, responses to this challenge are also beginning to develop, albeit with varying approaches. Japan and South Korea are two of the leading countries in East Asia in drafting national policies on artificial intelligence that balance technological innovation and the protection of individual rights. Japan's *"Artificial Intelligence Strategy 2021"* focuses on the ethical and responsible application of artificial intelligence, including promoting a supervisory system for the automated processing of personal data. South Korea, with its *"Framework Act on Intelligent Informatization,"* has also established principles for the protection of personal data in digital ecosystems controlled by artificial intelligence systems. In the Southeast Asian region, developments are quite diverse. Singapore pioneered the implementation of a comprehensive data protection law through the Personal Data Protection Act (PDPA), which also regulates the principles of responsibility and clarity in data processing using artificial intelligence systems. Malaysia and Thailand have also introduced personal data protection regulations, although they have not specifically regulated the framework for the use of artificial intelligence. Meanwhile, developing countries such as Indonesia, Vietnam, and the Philippines are still in the transition phase toward formulating policies that are able to address the challenges of artificial intelligence as a whole.

Law No. 27 of 2022 on Personal Data Protection, created in Indonesia, is a significant step in meeting the legal requirements for data protection in the digital age. This clause is the first piece of legislation that expressly governs the rights and responsibilities associated with processing personal data, including the roles of data controllers, data processors, and data subjects. However, the use of artificial intelligence in data management has not been specifically regulated by the Personal Data Protection Law, either in terms of ethical standards, accountability principles, or algorithmic control mechanisms. The absence of specific legal norms on artificial intelligence in the Personal Data Protection Law creates a gap in legal supervision, especially in the context of automated decision-making, profiling, and algorithm-based mass surveillance.

The phenomenon of using artificial intelligence in Indonesia has grown rapidly in both the public and private sectors. In the financial sector, banks and financial technology (fintech) companies are using artificial intelligence algorithms for creditworthiness assessment, fraud detection, and customer service. In the healthcare sector, artificial intelligence systems are used to diagnose diseases through big data. In the e-commerce and social media sectors, artificial intelligence-based recommendation systems manage user preferences based on search and transaction history. In the government sector, the use of facial recognition technology and population data processing is increasing for administrative and national security purposes. Unfortunately, there are no specific regulations that ensure that the processing of personal data through artificial intelligence systems takes place in accordance with the principles of transparency, fairness, and legal accountability.

The massive penetration of artificial intelligence in Indonesian society, in the absence of a specific and technical legal framework, creates complex legal challenges. For example, people are often unaware that their personal data has been processed by automated systems, and many are even unaware of the consequences of such processing. This is contrary to the principle of informed consent and individual control over their personal data. Additionally, artificial intelligence systems used inaccurately can lead to discrimination, mislabeling, and adverse decision-making without a clear legal basis.

Studying artificial intelligence's function in the Personal Data Protection Law's implementation is crucial and urgent. There is legal uncertainty surrounding the standards of accountability, transparency, and fairness in the use of such technology. Due to the absence of precise and thorough restrictions in Law No. 27 of 2022 on Personal Data Protection regulating the processing of personal data by artificial intelligence systems, automated decision-making, in particular, has the potential to breach the rights of data subjects, whereas the development of digital technology in Indonesia has shown that artificial intelligence is increasingly massively used by both the public and private sectors in the management of people's personal data without an adequate legal supervision mechanism.

Al-Ghamdi et al. (2023) examined the ethical challenges posed by AI in personal data processing, emphasizing the need for transparency and fairness. However, their research primarily focuses on the theoretical implications of AI technology rather than its practical application within existing legal frameworks. On the other hand, Mahmud (2022) explored the legal implications of AI usage in Southeast Asia, focusing on regulatory gaps in the region. While this study highlights the inadequacy of current laws, it does not fully address the implications of AI for data protection within national legal systems, particularly in Indonesia. This study aims to evaluate the current state of AI regulation within Indonesia’s Personal Data Protection Law, identify key legal challenges, and recommend strategies for strengthening the legal framework to ensure transparency, fairness, and accountability. The findings of this study will contribute to the development of better legal practices in managing AI-based personal data processing, aligning Indonesia’s legal framework with global standards and protecting individual privacy rights in the digital age.

METHOD

In order to examine the favorable legal standards applicable to the use of artificial intelligence in Indonesia's personal data management, this study employed a normative legal research methodology. This normative or doctrinal research is based on a literature review that inventories relevant laws and regulations, legal theories, doctrines, and court decisions to address the formulation of the problem regarding the extent to which positive law, especially Law Number 27 of 2022 concerning Personal Data Protection, can regulate and supervise the use of artificial intelligence in an accountable and equitable manner. The approaches used are the statutory approach and the analytical approach.

The provisions of the Personal Data Protection Law, its implementing rules, and further data protection-related laws, along with the application of artificial intelligence technology, are examined using the statutory approach, both at the national and international levels. Meanwhile, the analytical approach is used to critically examine the substance of existing norms in relation to the practice of using artificial intelligence in personal data processing in Indonesia, including assessing legal gaps that arise due to the absence of technical rules related to algorithms, transparency principles, and system accountability. Laws and regulations serve as primary legal materials for this study, while legal literature serves as a secondary source, along with scientific journals and opinions from technology law experts. With this approach, this research aims to provide systematic legal arguments in addressing the contemporary challenges of data protection in the digital era and automation.

RESULT AND DISCUSSION

The Role of Artificial Intelligence in the Implementation of Personal Data Protection Law in Indonesia

The legal system has undergone significant change in the past 20 years due to the advancement of digital technology, particularly with regard to the protection of personal data. Artificial intelligence has emerged as a disruptive technology that directly affects the regulation of personal data in the context of information globalization. In addition to enhancing information technology's efficiency and capabilities, the integration of artificial intelligence into data management systems presents significant legal issues with regard to accountability, transparency, and human rights protection. The implementation of Law No. 27 of 2022 on Personal Data Protection, which serves as the legal basis for safeguarding citizen data in the digital age, has made these issues much more complicated in the Indonesian setting. Thus, a key issue that requires careful research is the connection between the application of the Personal Data Protection Law and the function of artificial intelligence.

As the public and private sectors rapidly digitize, the necessity for personal data protection grew, leading to the creation of the Personal Data Protection Law. The law establishes fundamental principles such as data subject consent, purpose limitation, accuracy, and data security. However, the application of these principles in practice faces complex dynamics, especially when artificial intelligence is used in the process of collecting, processing, and storing personal data. Artificial intelligence has the ability to perform large-scale data analysis at high speed, which can improve the efficiency of public and commercial services, but also poses very serious potential for abuse and privacy violations (Darono, 2020; Kogan et al., 2019; Putu Mega Juli Semara Putra et al., 2019). Therefore, the utilization of artificial intelligence must be accompanied by the strengthening of legal instruments and adequate technical regulations to avoid a legal vacuum in the implementation of the Personal Data Protection Law.

As stated in Article 28G, paragraph (1) of the 1945 Constitution of the Republic of Indonesia, the Personal Data Protection Law not only addresses the pervasive digital transformation in the public and private sectors, but it also represents the state's recognition of the right to privacy as a component of human rights. This Personal Data Protection Law normatively formulates the core principles of personal data protection that are in line with international norms, such as the General Data Protection Regulation (GDPR) of the European Union. These guidelines include the explicit agreement of the data subject and the particular goal of processing, data accuracy and updating, retention limitation, as well as the principles of data security and confidentiality (Richarde et al., 2023; Shen et al., 2023).

One important article that emphasizes the implementation of these principles is Article 20 of the Personal Data Protection Law, which requires personal data controllers to ensure that data processing is carried out on a legitimate basis, transparently, accountably, and in accordance with the original purpose for which it was collected. This provision explicitly states that personal data can only be processed for a purpose that has been explicitly disclosed to the data subject, and that the data controller must seek the data subject's consent again if the purpose changes. As a result, it is acknowledged that data processing cannot be done arbitrarily and that the data subject retains legal control over their personal information, not the controller or any other entity that collects or processes it the personal data. This provision is a concrete manifestation of the principles of purpose limitation and informed consent as recognized in the GDPR, while emphasizing the importance of protecting the authority of individuals over their personal data.

In practice, artificial intelligence systems are often used by the public and private sectors in Indonesia for various purposes, such as biometric identification, user profiling, recommendation systems, and fraud detection. This use has the potential to erode the rights of data subjects if it is not accompanied by the principles of accountability and clarity of algorithms. Unfortunately, the Personal Data Protection Law does not explicitly regulate ethical or technical standards in the use of artificial intelligence for personal data processing. This creates a significant legal loophole, given that artificial intelligence can make inferences and predictions that data owners are not always aware of, including accessing sensitive data such as location, health, and a person's political and sexual orientation. In this context, legal protection of personal data becomes very vulnerable if there is no clear supervision and accountability mechanism for artificial intelligence systems.

The principle of accountability enshrined in Law No. 27 of 2022 on Personal Data Protection should not be narrowly understood as an administrative obligation to record, report, or maintain data security, but rather expanded into a form of substantial legal responsibility, particularly when harm arises from the use of artificial intelligence-based systems. In this context, the principle of accountability should emphasize liability for the legal consequences of automated decisions or algorithmic data processing that impact the rights of data subjects, including violations of privacy rights, unfair profiling, or discriminatory decisions generated by artificial intelligence systems.

In contemporary legal theory, particularly in the framework of strict liability and vicarious liability, legal liability for harm caused by smart technology cannot only be imposed on end users or owners of personal data, but must cover the entire digital ecosystem (Silva et al., 2016). This includes technology providers, algorithm system developers, digital platform providers, as well as data control institutions that take strategic decisions over the processing of personal data. This view is based on the principle of risk allocation, namely that the actor with the most technical capability and control over the risk should also bear legal responsibility when the risk becomes a legal reality that harms the data subject (Mitrakas, 2011).

However, a major challenge in the Indonesian context is that there is no technical regulatory tool or legal liability framework that explicitly regulates the division of liability in the event of a data breach or negative impact due to automated decisions from algorithms. The opaque and technically complex nature of artificial intelligence systems makes it difficult to identify the most responsible actor. As a result, the principle of accountability in the Risk Protection Law has become normative without a clear execution mechanism.

In some developed jurisdictions such as the European Union, Japan, and South Korea, the “explainable AI” (XAI) approach is beginning to be developed as a legal principle that aims Artificial intelligence (AI) systems that make decisions that affect people must be able to clearly explain the algorithmic reasoning behind their choices. This idea is a component of the transition from a reactive legal framework to a preventive and transparent model, which emphasizes not only the protection of personal data post-breach, but also on ex-ante transparency obligations that allow data subjects to understand, challenge or correct algorithmic decisions.

Indonesia can adopt the explainable principle of artificial intelligence in the implementation of the Protection Law as part of the mechanism to strengthen the principle of legal accountability. The implementation of this principle can be regulated in implementing regulations or technical standards that require entities using artificial intelligence systems to provide reasonable explanations for system decisions, algorithmic audits, as well as the obligation to disclose the predictive models used, especially if the resulting decisions have a direct impact on the rights of data subjects, such as in financial services, law enforcement, or social assistance distribution. In this way, Indonesia not only strengthens its data protection regime, but also ensures that artificial intelligence-based digital transformation remains within the control of the law based on the principles of fairness and protection of human rights.

This phenomenon is not only happening in Indonesia, but is also a regional concern in Southeast Asia. Countries such as Singapore and Malaysia have developed personal data regulations that incorporate the principle of ethical and transparent use of artificial intelligence. Singapore, for example, through the Personal Data Protection Commission (PDPC), has published guidelines for the responsible use of artificial intelligence, including the need for algorithm documentation, data audits, and public participation in the oversight of digital systems (Abiteboul & Stoyanovich, 2019). These steps provide important lessons for Indonesia in formulating derivative policies from the Protection Law that specifically regulate the use of artificial intelligence in information systems.

The global phenomenon also shows that the use of artificial intelligence in personal data management has led to various legal disputes that reflect the urgency of more detailed regulation. In the European Union, for example, the Cambridge Analytica case has sparked a debate on the ethical and legal limits of the use of personal data by artificial intelligence systems. Similarly, in the United States, artificial intelligence-based facial recognition systems have been criticized for their high risk of racial discrimination and violation of privacy rights (Setiawan & al., 2021). These cases show that artificial intelligence is not only a technological tool, but also an entity that can have legal repercussions if not controlled through effective regulatory tools.

In the Indonesian context, the implementation of Law No. 27 of 2022 on Personal Data Protection still faces serious challenges, especially in terms of structural and institutional readiness to respond to the development of artificial intelligence-based technology. While the An independent supervisory authority has been established under the Protection Law to monitor adherence to the standards of protecting personal data, it has yet to be functionally established and is still at the institutional formulation stage. This has a direct impact on the absence of technical tools, algorithmic auditing systems, digital system monitoring protocols, and reliable data dispute resolution mechanisms in the context of the use of artificial intelligence.

As Nasution (2023) points out, a major challenge in personal data protection in Indonesia lies in the "asymmetry of capability between regulators and technology developers", where technology developers are moving very fast, while the country's institutional structures are still slow in building the legal and technical capacity to supervise (L. Li et al., 2019; Malatji et al., 2021; Rizal & Yani, 2016; Snider et al., 2021). I This is in line with the findings of Budiati and Gunawan (2022) in an empirical study showing that the majority of government agencies do not yet have specialized units or personnel with sufficient digital competencies to handle the legal implications of automation systems and artificial intelligence-based data processing. Furthermore, according to Irene Joe and Sinta Dewi (2021), another challenge that exacerbates the situation is the low legal and technological literacy among policy makers and law enforcement. Many of them do not understand the complexity of algorithmic systems, especially regarding how automated decision-making can impact the rights of data subjects, including the risk of discriminatory profiling, violation of the principle of fairness, and algorithm bias (Belenguer, 2022). This is exacerbated by the general public's lack of understanding of their rights to personal data, leading to weak or non-use of grievance mechanisms and resistance to data abuse.

Referring to international practices, such as that of the European Data Protection Board (EDPB), this challenge is addressed by building an institutional structure equipped with specialized technical divisions for artificial intelligence oversight, algorithm auditing, and systemic risk monitoring of new technologies. Supervisory institutions in Europe not only consist of legal experts, but also recruit data scientists, ethical technologists, and engineers to ensure that oversight of artificial intelligence-based data processing is not formalistic, but substantive and based on technical analysis. Therefore, a comprehensive national strategy is needed, not only in the form of regulations, but also institutional capacity building, structural reforms, and large investments in strengthening human resources and legal technology.

This strategy should include: (1). Accelerating the establishment and strengthening of data protection authority institutions, (2). Preparation of technical guidelines for the supervision of artificial intelligence systems, (3). Legal and technological literacy programs for law enforcement and policy makers, and (4). Establishment of a national framework for algorithm auditing and ethical AI governance. As Lawrence Lessig stated, “code is law”, meaning that software and algorithms now have the same power as written law in shaping people's behavior (W. Li & al., 2015). Therefore, the state must be present not only as a passive regulator, but as an architect of digital regulation that is able to build an adaptive, predictive and proactive legal system in the face of the artificial intelligence technology revolution.

This regulatory limitation is also evident from the absence of implementing regulations that specifically regulate how artificial intelligence can and cannot be used in the context of personal data management. The absence of technical standards or audit procedures creates a confusing gray area for both technology industry players and law enforcement. In this case, derivative regulations are needed that regulate the principles of fairness, explainability, and accountability, as a legal basis for all personal data processing activities using artificial intelligence. Thus, the rights of data subjects can be optimally protected and the risk of data misuse can be minimized.

Moreover, the legal discourse on artificial intelligence in the management of personal data must consider aspects of fundamental human rights, including the right to privacy, the right not to be discriminated against, and the right to be informed. Within the framework of human rights, every individual has the right to know how his or her personal data is used, including whether the decisions taken by artificial intelligence systems can be legally and ethically justified. Artificial intelligence technology used to collect, analyze, and make decisions based on personal data directly touches fundamental aspects of human dignity, especially the right to privacy, the right not to be discriminated against, and the right to correct and accessible information. This makes it insufficient for the regulation of artificial intelligence to be based solely on the principles of efficiency and innovation, but must be subject to a universal and non-derogable human rights framework.

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) guarantees that no one will be subjected to arbitrary or unlawful interference with his private life, family, household, or correspondence. The right to legal defense against such meddling is part of this. In this sense, it might be argued that the processing of personal data by artificial intelligence without strict control and accountability rules violates the right to privacy protected by both international legal agreements and Article 28G paragraph (1) of the 1945 Constitution.

The use of AI in decision-making such as in financial services, education, or the justice system poses a risk of algorithmic discrimination, especially if the training data contains historical or structural biases. As Sandra Wachter and Brent Mittelstadt of the Oxford Internet Institute have argued, there is a systemic risk that AI can lead to “black box decisions”, i.e. decisions that humans cannot trace the logic of, thereby inhibiting the right of individuals to understand and challenge decisions that impact their lives (Elliott & al., 2021). In Indonesian regulations, especially in the Personal Data Protection Law, there is no explicit mention of the right to an explanation or the right to object to an automated decision, but these principles can be interpreted as part of the rights of data subjects that must be guaranteed by the state, especially through the implementation of derivative policies and technical regulations.

The Indonesian government must make sure that the Personal Data Protection Law is implemented in a way that not only conforms with national legal requirements but also with international human rights protection principles. According to former UN Special Rapporteur on Freedom of Opinion and Expression David Kaye, nations that regulate AI need "ground human rights principles in the design, development and application of artificial intelligence from the outset, not as a later reflection."

This research shows that the role of artificial intelligence in the implementation of personal data protection law in Indonesia is ambivalent. On the one hand, artificial intelligence offers great opportunities to strengthen the efficiency and accuracy of information systems that manage personal data. On the other hand, without strict legal supervision and regulation, artificial intelligence can become a very dangerous instrument of human rights violations. It should be emphasized that the successful implementation of the Protection Law in the era of artificial intelligence is highly dependent on the state's ability to develop a legal framework that is responsive and adaptive to technological dynamics. Strengthening institutional capacity, developing technical regulations, and improving people's legal and digital literacy are crucial elements in ensuring that the role of artificial intelligence truly becomes a complement, not a threat, to the legal system of personal data protection in Indonesia.

Legal Certainty of the Use of Artificial Intelligence Technology in Personal Data Management Based on Personal Data Protection Law in Indonesia

Artificial intelligence has become a transformational force in various sectors, including in the realm of law and management of personal data. The passage of Law No. 27 of 2022 on Personal Data Protection in Indonesia represents a significant turning point in the country's efforts to establish data governance that is fair, open, and responsible. Within the Protection Law's implementation framework, artificial intelligence has two main roles: first, as an instrument that strengthens supervision and enforcement of personal data protection; second, as a technology that inherently poses new legal challenges that need to be anticipated by the national legal system. The first role places artificial intelligence as a tool that supports personal data oversight institutions, such as the Personal Data Protection Authority, in identifying data breaches, analyzing data usage patterns, and predicting potential risks of information leakage in real-time. Through machine learning, natural language processing (NLP), and big data analytics technologies, artificial intelligence can be used to detect behavioral anomalies in data management systems, monitor compliance with privacy policies, and provide early warning of possible data subject rights violations (Ardabili & al., 2023).

In this context, artificial intelligence acts as a catalyst for regulatory effectiveness. This function is in line with the spirit of the Protection Law, which prioritizes the principles of law enforcement and compliance monitoring. Articles in the Protection Law regulate the obligations of data controllers and processors, the rights of data subjects, as well as dispute resolution mechanisms and administrative and criminal sanctions. The role of artificial intelligence does not stop at being a regulatory tool. As a technology that has the ability to learn, adapt and make decisions autonomously, artificial intelligence also presents its own legal complexities. This is where the second role of artificial intelligence lies, namely as a legal object that has the potential to cause conflicts between technological efficiency and the human right to privacy. The use of artificial intelligence in recommendation systems, facial recognition, mass surveillance, and social rating systems can lead to serious privacy violations if not strictly regulated (Ameen et al., 2012).

Legal certainty is a central issue, so the Protection Law seeks to create a clear and predictable legal space, but the rapid development of artificial intelligence demands regulatory flexibility and adaptability. The main challenge faced is how to develop legal norms that not only regulate current phenomena, but are also able to anticipate future technological developments. As a result, it is vital to regulate artificial intelligence using principles. The development and application of artificial intelligence in the area of personal data can be ethically and legally supported by a protection law that upholds values like accountability, justice, transparency, and data minimization.

In the context of personal data regulation and digital technology, legal certainty is a central issue that must be faced by policymakers. Law No. 27 of 2022 on Personal Data Protection was born as an instrument to create a clear, structured, and predictable legal space, especially in the face of rapid digital transformation in the public and private sectors. However, as expressed by Eddy Damian, states that: Legal certainty is not only a matter of normative clarity, but also related to the ability of the law to respond to evolving social and technological dynamics, including the phenomenon of artificial intelligence which is currently a disruptive force in personal data management (Bukit & Ayunda, 2022).

The exponential and non-linear development of artificial intelligence poses a dilemma in legal construction: on the one hand, the law is required to ensure predictability and protection of rights, but on the other hand, the law must also be adaptive to changing technology. This was emphasized by Sinta Dewi Rosadi, a cyber law expert from Padjadjaran University, who stated that: “The law on personal data protection should not be rigid, but should open a space for regulatory adaptation that allows responses to new technologies such as artificial intelligence, cloud computing, and big data.”

In this context, the principle-based regulation approach becomes very relevant. Instead of strictly regulating specific behaviors that quickly become obsolete, this approach emphasizes general principles such as accountability, transparency, fairness, prudence, and data minimization as a flexible yet binding normative foundation. This approach is in line with the international practice applied in the European Union's General Data Protection Regulation (GDPR), which also emphasizes the importance of general principles as guidelines in building an artificial intelligence-based personal data governance system. Indonesia through the Protection Law has begun to adopt this approach, as reflected in a number of principles contained in these provisions such as: Principles of Accountability; Principles of Justice and Legal Certainty; Principles of Transparency; Principles of Purpose Limitation and Data Minimization.

Benny Riyanto has also argued for this principled approach, highlighting the need for future digital regulations to combine the idea of legal certainty with the capacity to foresee technological change. This means that the government must create regulations based on universal legal ethical principles rather than merely technical regulations that are quickly rendered obsolete. This type of law is both futuristic and constitutional (Ranchordás & Van‘t Schip, 2020). The main obstacle, though, is putting these ideas into practice through particular institutional and technical rules, such as reporting requirements for AI service providers that handle personal data, algorithm audit processes, and ethical guidelines for AI use. The principles will only be moral statements with no legal weight if there are no effective tools to put them into practice.

The creation of inclusive and equitable data governance is also linked to the incorporation of artificial intelligence in the application of the Protection Law. Fairness and nondiscrimination must be the foundation for the development and application of artificial intelligence. In reality, if artificial intelligence algorithms are not properly created, they may replicate or even strengthen preexisting social biases. Therefore, an algorithmic review mechanism must be incorporated into the Protection Law's structure in order to test the transparency, rationale, and influence on individual rights of any decision-making process made by artificial intelligence systems.

However, stringent technological and procedural criteria are also required to enhance the legal protection of personal data processed by AI systems. The legal-technological infrastructure that needs to be established includes cybersecurity audits, certification of AI systems, and standardization of encryption protocols. The fundamental tenets of contemporary data regulation security by design and privacy by default will be reinforced as a result (P et al., 2023). The obligation for artificial intelligence technology providers to conduct data protection impact assessments before launching new systems is an important instrument in preventing systemic data breaches.

Enhancing human resources in the domains of technology and law is also necessary for the Protection Law's artificial intelligence implementation. To adequately evaluate the possible hazards, law enforcement officials, regulators, and data controllers need to have a solid grasp of how artificial intelligence systems operate. To close the gap between the legal profession and technological advancement, interdisciplinary training and technology-based legal education are desperately needed.

The creation of a digital ecosystem built on trust must be the ultimate goal of the cooperation between laws protecting personal information and the advancement of artificial intelligence technology. A number of parties, including the public and corporate sectors, academia, and civil society, must actively participate in this. An efficient data protection system may be made possible by artificial intelligence, but if it is not handled responsibly and responsibly, it may potentially become a major threat.

Thus, artificial intelligence plays a multifaceted and intricate role in Indonesia's application of the Protection Law. Artificial intelligence can be used as a strategic partner to improve law enforcement, oversight, and prevention of infractions involving personal data. However, in order to preserve the values of human rights protection in the digital age, artificial intelligence also necessitates a progressive and adaptable legal reconstruction. Only until technological, normative, and institutional factors are in balance will there be legal certainty on the use of AI in the management of personal data. The Protection Law serves as the first pillar of the regulatory system; nonetheless, it will be difficult to maintain the law's applicability, flexibility, and humanity in the face of the rapidly changing digital landscape.

As a result, a future-focused regulatory approach is required that can keep up with technical advancements without sacrificing the fundamental principles of protecting personal information. This plan calls for improving algorithmic openness, bolstering technology-based oversight, creating accountability systems, and guaranteeing public involvement in the regulatory process. With a sizable population that uses technology, Indonesia has a fantastic chance to lead the way in the creation of artificial intelligence governance grounded in social justice and human rights. Artificial intelligence's involvement in the Protection Law's implementation is not solely a technological one; it also concerns how the law adapts to contemporary issues while maintaining its foundation in human dignity.

CONCLUSION

Artificial intelligence's role in enforcing Law No. 27 of 2022 on the Protection of Personal Data in Indonesia presents both opportunities for efficiency and serious challenges in guaranteeing individual privacy rights. While the law has adopted data protection principles in line with international standards, the lack of technical regulations and accountability mechanisms for the use of artificial intelligence creates significant legal gaps. Therefore, institutional strengthening, algorithmic oversight, and the adoption of explainable principles of artificial intelligence are urgent needs to ensure that the processing of personal data remains under the control of the law that upholds human rights. Legal certainty regarding the use of artificial intelligence in personal data management in Indonesia requires adaptive, principle-based, and human rights-based regulations. Law No. 27 of 2022 has laid the initial groundwork but still needs to be supported by technical instruments, algorithmic accountability, and strengthened institutional capacity. Artificial intelligence must be regulated not only as a tool for law enforcement but also as a technological entity with potential risks, requiring responsive, transparent, and humane governance.

REFERENCES

Abiteboul, S., & Stoyanovich, J. (2019). Transparency, Fairness, Data Protection, Neutrality: Data Management Challenges in the Face of New Regulation. *Journal of Data and Information Quality (JDIQ)*, *11*(3), 1–9.

Ameen, M. Al, Liu, J., & Kwak, K. (2012). Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications. *Journal of Medical Systems*, *36*, 93–101.

Ardabili, B. R., & al., et. (2023). Understanding Policy and Technical Aspects of Ai-Enabled Smart Video Surveillance to Address Public Safety. *Computational Urban Science*, *3*(1), 21.

Belenguer, L. (2022). AI Bias: Exploring Discriminatory Algorithmic Decision-Making Models and the Application of Possible Machine-Centric Solutions Adapted from the Pharmaceutical Industry. *AI and Ethics*, *2*(4), 771–787.

Bukit, A. N., & Ayunda, R. (2022). Urgensi Pengesahan RUU Perlindungan Data Pribadi Terhadap Perlindungan Kebocoran Data Penerimaan SMS Dana Cepat. *Reformasi Hukum*, *26*(1), 1–20. https://doi.org/10.46257/jrh.v26i1.376

Darono, A. (2020). Web Data Extraction Dalam Analitika Data Audit: Pengembangan Artefak Teknologi Dalam Perspektif Design Science Research. *Teknika*, *9*(2), 97–105. https://doi.org/10.34148/teknika.v9i2.283

Elliott, K., & al., et. (2021). Towards an Equitable Digital Society: Artificial Intelligence (AI) and Corporate Digital Responsibility (CDR). *Society*, *58*(3), 179–188.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*. https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Li, W., & al., et. (2015). Law Is Code: A Software Engineering Approach to Analyzing the United States Code. *J. Bus. & Tech. L.*, *10*, 297.

Malatji, M., Marnewick, A. L., & von Solms, S. (2021). Cybersecurity policy and the legislative context of the water and wastewater sector in South Africa. *Sustainability (Switzerland)*, *13*(1). https://doi.org/10.3390/su13010291

Mitrakas, A. (2011). Assessing Liability Arising from Information Security Breaches in Data Privacy. *International Data Privacy Law*, *1*(2), 129–136. https://doi.org/10.1093/idpl/ipr001

P, A. A. W., Esfandiari, F., & Wasis. (2023). Juridical Analysis of Legal Protection of Personal Data in Terms of Legal Certainty. *Indonesia Law Reform Journal*, *3*(1), 96–108. https://doi.org/10.22219/ilrej.v3i1.23840

Ranchordás, S., & Van't Schip, M. (2020a). Future-Proofing Legislation for the Digital Age. In *Time, Law, and Change: An Interdisciplinary Study*. https://doi.org/10.5040/9781509930968.ch-016

Ranchordás, S., & Van't Schip, M. (2020b). Future-Proofing Legislation for the Digital Age. In *Time, Law, and Change: An Interdisciplinary Study*. https://doi.org/10.5040/9781509930968.ch-016

Richarde, A. P. M., Prado, P. H. M., & Ferreira, J. B. (2023). Privacy Signals: Exploring the Relationship between Cookies and Online Purchase Intention. *Revista de Administracao Contemporanea*, *27*(4). https://doi.org/10.1590/1982-7849rac2023220311.por

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1), 61. https://doi.org/10.21512/jas.v4i1.967

Setiawan, D., & al., et. (2021). Implementasi Convolutional Neural Network Untuk Facial Recognition. *Media Informatika*, *20*(2), 66–79. https://doi.org/10.37595/mediainfo.v20i2.68

Shen, A., Francisco, L., Sen, S., & Tewari, A. (2023). Exploring the Relationship between Privacy and Utility in Mobile Health: Algorithm Development and Validation via Simulations of Federated Learning, Differential Privacy, and External Attacks. *Journal of Medical Internet Research*, *25*. https://doi.org/10.2196/43664

Silva, S. N., Reed, C., & Kennedy, E. (2016). *Responsibility, Autonomy and Accountability: Legal Liability for Machine Learning*. *243*, 1–31.

Snider, K. L. G., Shandler, R., Zandani, S., & Canetti, D. (2021). Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab019