International Journal of Social and Education (INJOSEDU) https://languar.net/index.php/INJOSEDU
Vol. 3 No. 2 May 2026, hal., 168-182 e-ISSN: 3047-6151

LEGAL TRANSFORMATION IN THE AGE OF ARTIFICIAL INTELLIGENCE: A LITERATURE REVIEW ON REGULATORY, ETHICAL AND DATA PROTECTION CHALLENGES IN INDONESIA

Gunawan Widjaja
Senior Lecturer, Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Abstract

The exponential development of artificial intelligence (AI) has created a fundamental disruption to the national legal order, demanding regulatory transformation that is adaptive to algorithmic autonomy, ethical issues, and the protection of personal data. This article aims to analyse the legal challenges faced by Indonesia in the AI era through a literature *review* using a juridical-normative approach and content analysis. The research findings indicate that Indonesia faces a specific regulatory vacuum (*legal vacuum*) that creates legal uncertainty, particularly regarding liability for discriminatory or harmful AI decisions resulting from the lack of transparency associated with the *'black box'* problem. Fragmented inter-institutional authority and the regulatory body's lack of technical expertise exacerbate the situation, whilst the implementation of Law No. 27 of 2022 on Personal Data Protection (PDP Law) faces technical dilemmas regarding data minimisation, *informed consent*, and *the right to erasure* within *machine learning* systems. From an ethical perspective, algorithmic bias has the potential to perpetuate structural discrimination that runs counter to the values of Pancasila, whilst the absence of an obligation to label synthetic content threatens the integrity of public information. This article recommends the enactment of a dedicated AI law adopting the principle of *strict liability*, strengthening the capacity of the Personal Data Protection Agency, formulating operational AI ethics grounded in Pancasila, and implementing a hybrid legal approach combining *hard law* with *soft law*. This legal transformation is an absolute prerequisite for Indonesia to harness the potential of AI for Indonesia Emas 2045 without compromising human rights, social justice, and the nation's digital sovereignty.

Keywords: artificial intelligence, legal transformation, regulatory challenges, AI ethics, personal data protection, Indonesia.

Introduction

The Fourth Industrial Revolution has transformed *artificial* intelligence (AI) from the realm of science fiction into a fundamental infrastructure driving the global digital economy, including in Indonesia. The adoption of AI in Indonesia has seen a significant surge, positioning the country as a leader in the Southeast Asian region in terms of the level of smart technology usage, although for the most part it still functions as a consumer of technology rather than a producer of innovation (Ridhwan, 2025). This transformation is not only reshaping the business and industrial landscape, but also overhauling the social, political and legal frameworks that have long formed the

foundation of state life. The existence of algorithms capable of independent learning (*machine learning*) and autonomous decision-making demands a reconstruction of the legal paradigm previously designed for conventional human interaction.

The Indonesian government has responded to this wave of disruption by publishing the National Artificial Intelligence Strategy (Stranas KA) 2020–2045, which sets out five key priority areas: public services, health, bureaucratic reform, education and research, and food security (Indonesia, 2020) . This strategic document serves as an initial guide for the integration of AI into national development; however, as it remains a policy guideline (*soft law*), it lacks the strong legal binding force to enforce compliance or impose sanctions for violations. The absence of specific legislation governing the AI ecosystem creates *a legal vacuum* that is potentially open to abuse, particularly when this technology is used in crucial public decision-making that has far-reaching implications for human rights.

The complexity of legal challenges reaches a peak when AI systems begin to be used in sensitive areas, such as workforce recruitment, banking credit assessments, medical diagnosis and predictive law enforcement. In this context, fundamental questions arise regarding legal accountability: who should be held responsible when algorithms make decisions that are discriminatory, harmful, or even fatal to human life? Contemporary cyber law literature indicates that the current *product liability* regime is insufficient to address the dynamic and often non-transparent nature of AI's autonomy—a phenomenon known as *the 'black box* problem' (Cohen, 2019) . The inability to trace the decision-making logic of these algorithms poses a serious obstacle to the enforcement of both restorative and retributive justice in Indonesia.

In addition to accountability issues, the integration of AI also poses systemic risks to privacy and the protection of personal data, given that the primary fuel for AI operations is massive amounts of data (*big data*). Indonesia has, in fact, taken a step forward by enacting Law No. 27 of 2022 on Personal Data Protection (PDP Law), which adopts universal principles such as transparency, purpose limitation, and accountability (Government of the Republic of Indonesia, 2022). However, the implementation of the PDP Act within the AI ecosystem faces serious technical and legal challenges, particularly regarding *consent* mechanisms—which are often not fully understood by data subjects—as well as difficulties in applying *the right to be forgotten* to AI models that have 'learned' from such data. This ambiguity creates a legal loophole that can be exploited by businesses to process data excessively for the purpose of training their AI models.

From an ethical perspective, the use of AI in Indonesia also faces significant challenges regarding algorithmic bias, which can reinforce entrenched social stereotypes, racial discrimination and gender inequality. Global and local case studies show that non-representative *training data* often produces biased AI outputs, which are then legitimised by the perceived objectivity of the machine (Valdivia, 2018) . In

Indonesia, with its highly complex demographic and cultural diversity, the risk of such bias is heightened if AI development is dominated by a handful of developers from homogeneous backgrounds without strict ethical oversight. Without regulatory intervention mandating ethical audits and data diversity, AI technology risks becoming a new tool of oppression that marginalises vulnerable groups.

This regulatory gap is exacerbated by the pace of technological innovation, which far outstrips that of traditional legislation—a phenomenon known as *the 'pacing problem'* in the study of technology law. Whilst legislators require years to draft, debate and enact a single regulation, AI development cycles run in a matter of months, weeks (Acemoglu & Restrepo, 2020) . This lag often leaves Indonesian law in a reactive position, responding only after violations or scandals have occurred, rather than being proactive enough to prevent risks from the design stage (*privacy and ethics by design*). A rigid and static legal approach is clearly no longer relevant for regulating fluid, adaptive, and constantly evolving technologies such as AI.

At the global level, the European Union has already established the gold standard for AI regulation through *the EU AI Act,* which classifies AI risks and imposes strict bans on certain uses deemed to threaten fundamental rights (Act, 2024) . Singapore, as Indonesia's close neighbour, has also released *a testing framework* and pragmatic ethical guidelines to encourage innovation whilst mitigating risks (Yuliana & Anita, 2026) . Indonesia's current lack of specific AI regulations risks turning the country into *a 'regulatory haven'* for foreign AI developers seeking to avoid strict ethical standards, or conversely, could hinder investment due to legal uncertainty. Harmonisation with international standards is essential to ensure Indonesia does not fall behind in a global digital economy increasingly fragmented by differing regulatory standards.

This challenge of legal transformation also touches upon aspects of digital sovereignty and national security, given Indonesia's extremely high dependence on foreign-made AI infrastructure and models. Recent reports indicate that although AI adoption in Indonesia is very high, its production capacity and ownership of core technology remain minimal, meaning the country functions more as a consumer market than a key player(Purbasari et al., 2025) . This dependence creates strategic vulnerabilities, whereby critical decisions affecting the livelihoods of many people can be controlled by algorithms whose servers and logic reside within the jurisdiction of another country. Legal reform must address this challenge to data sovereignty by mandating *data* localisation or, at the very least, ensuring secure and auditable cross-border data transfer mechanisms.

In the academic sphere, the discourse on law and AI in Indonesia remains fragmented and has yet to produce a comprehensive theoretical synthesis to guide policymakers. Most of the existing literature tends to focus on technical aspects of computer science or superficial analyses of the ITE Law and the PDP Law without

thoroughly examining the philosophical and sociological implications of machine autonomy (Li et al., 2025) . There is an urgent need for in-depth literature analysis to map regulatory gaps, identify ethical principles relevant to the values of Pancasila, and formulate adaptive policy recommendations. This article aims to fill this gap in the literature by providing an intellectual roadmap for the transformation of AI law in Indonesia.

The urgency of this research becomes all the more apparent when considering current socio-political dynamics, in which *the* use of *generative AI* has flooded the public sphere with synthetic content that is difficult to distinguish from reality, raising the risk of disinformation and the destabilisation of democracy. The phenomenon of *deepfakes* and propaganda bots utilised in political contests demonstrates that threats to information integrity are no longer a conspiracy theory, but a legal reality that urgently requires regulation (Wardle & Derakhshan, 2017) . Indonesian law must evolve to be able to identify, track, and take action against the misuse of AI that threatens public order without infringing upon the freedom of expression guaranteed by the constitution. This balance between national security and civil rights represents one of the greatest challenges for legislators in the digital age.

Furthermore, legal transformation in the AI era is not merely about creating new rules, but also about building institutional capacity and human resources capable of enforcing them. Supervisory bodies, such as the newly established personal data protection authority, need to be equipped with robust technical expertise in algorithmic forensics and system auditing (Adnin et al., 2024) . Without adequate law enforcement infrastructure, even the most sophisticated regulations will merely be a 'paper tiger' lacking the teeth to stand up to the tech giants (*big tech*). Therefore, discussions on legal transformation must always be accompanied by strategies to strengthen institutional capacity and foster pentahelix collaboration between government, academia, industry, the community, and the media.

Based on the background outlined above, this article aims to conduct a critical literature review of legal transformation in Indonesia in the face of the artificial intelligence era, focusing on two main pillars: regulatory challenges and ethical issues, as well as data protection.

Research Methodology

This study employs a literature *review* method, utilising a legal-normative approach and qualitative content analysis to examine legal transformation in the era of artificial intelligence in Indonesia. Secondary data was collected through a systematic search of primary sources in the form of legislation (including the ITE Law, the PDP Law, and the 2020–2045 National Artificial Intelligence Strategy), and secondary sources in the form of textbooks, national journal articles and international journal articles(Walliman & Walliman, 2021). Data analysis was conducted using a legal comparison

method to compare Indonesia's regulatory framework with other jurisdictions such as the European Union and Singapore, as well as systematic interpretation to construct the coherence of existing legal norms with universal AI ethical principles. Data validity is ensured through source triangulation, whereby findings from one piece of literature are cross-verified with other independent sources to ensure the objectivity and accuracy of the analysis, thereby producing a comprehensive theoretical synthesis regarding regulatory gaps and policy recommendations relevant to the national legal context (Eliyah & Aslan, 2025) .

Results and Discussion

Regulatory Challenges in the Age of Artificial Intelligence

The most fundamental regulatory challenge facing Indonesia in the era of artificial intelligence is the absence of specific legislation that comprehensively governs the AI lifecycle, from research and development through to deployment and post-implementation audits. To date, the existing legal framework remains fragmented and scattered across various sectoral regulations, such as Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 on Electronic Information and Transactions (EIT Law) and the Circular Letter of the Minister of Communication and Information Technology No. 9 of 2023 on Artificial Intelligence Ethics, which is merely a moral appeal lacking enforceable sanctions(Sukmaningsih, 2025) . The absence of this primary legal framework (*omnibus law*) creates serious *legal uncertainty* for industry players, investors and the general public, thereby hindering innovation whilst opening the door to the misuse of technology that is detrimental to the public.

This regulatory vacuum becomes increasingly critical when it comes to the issue of legal *liability* for losses caused by autonomous AI decisions, a phenomenon known as *the accountability gap*. In the Indonesian civil law system, Article 1365 of the Civil Code (KUHPerdata) on Unlawful Acts (PMH) requires the element of fault as the basis for a claim; however, this requirement becomes extremely difficult to prove when AI algorithms operate through a *black-box* mechanism that is non-transparent even to their own developers (Li et al., 2025) . Recent legal literature emphasises that without a reformulation of the doctrine of *product liability* or the adoption of the principle of *strict liability* as mandated more explicitly in Article 1367 of the Civil Code, victims of AI errors will be trapped in a 'vacuum of liability' where no party can be held legally accountable (Ravizki & Yudhantaka, 2022) .

The complexity of regulatory challenges is increasing as AI is used in the public sector for administrative decision-making that directly impacts citizens' rights, such as determining recipients of social assistance, assessing staff performance, and predicting areas prone to crime. Recent studies indicate that the use of AI within Indonesia's bureaucracy is frequently carried out without a clear legal basis (*ultra vires*), without algorithmic audit mechanisms, and without effective administrative appeal channels for

citizens who feel aggrieved by machine-made decisions . This runs counter to the principle *of due process of law* and the principles of *good governance*, whereby every state decision must be traceable in terms of its legal and factual grounds (*reasoned decision*)—a standard that is difficult for probabilistic generative AI systems to meet.

From a criminal law perspective, the regulatory vacuum surrounding AI also creates confusion regarding the legal status of the perpetrator of a criminal offence when an autonomous system causes serious physical or material harm. Indonesian criminal law, as set out in the Criminal Code (KUHP), recognises only humans (*natural persons*) and corporations (*legal persons*) as legal subjects; consequently, robots or AI algorithms cannot be held criminally liable even if they directly cause fatal accidents (Sulistio & Salsabilla, 2023). This dilemma calls for an update to criminal law doctrine to accommodate the concept *of 'electronic personhood'* or, at the very least, to extend vicarious liability to the owners and developers of AI—a discourse that has yet to receive legislative certainty in Indonesia.

Regulatory challenges also arise in the form of a technical capacity gap between policymakers (*regulators*) and the pace of technological innovation (*innovators*), a global phenomenon known as *the 'pacing problem'*. Legislators and regulators in Indonesia often lack a deep technical understanding of AI architecture, *machine learning*, and their social implications, resulting in regulations that are too general, impractical, or even hinder innovation (Purbasari et al., 2025) . This skills gap is exacerbated by the lack of dedicated units focused on regulating emerging technologies within relevant ministries and agencies, leading to policy responses that are often reactive and piecemeal, only emerging after scandals or major breaches have occurred.

The fragmentation of authority across institutions constitutes another structural barrier that undermines the effectiveness of AI regulation in Indonesia, where overlapping jurisdictions between the Ministry of Communication and Digital Affairs, the National Cyber and Cryptography Agency, the Ministry of Law, and various technical ministries lead to policy inconsistencies. For example, AI security standards for the healthcare sector issued by the Ministry of Health may differ from those set by the Food and Drug Supervisory Agency (BPOM) or the National Cyber and Cryptography Agency (BSSN), thereby confusing industry players who must comply with non-harmonised regulations (Pradana et al., 2025) . Without a single coordinating body or a centralised *AI Regulatory Sandbox*, Indonesia's regulatory ecosystem will remain fragmented and unable to provide holistic legal certainty.

From a consumer protection perspective, current regulations are insufficient to protect users from manipulative practices such as AI-enhanced *dark patterns*, *dynamic pricing*, and the exploitation of behavioural data that infringes upon individual autonomy. Law No. 8 of 1999 on Consumer Protection , which serves as the primary legal basis, remains focused on conventional transactions and has not anticipated the

complexity of human-machine interactions on digital platforms (Respati, 2024) . The absence of a requirement for labelling synthetic content (*AI-generated content labelling*) also makes it difficult for consumers to distinguish between genuine information and deepfake fabrications, leaving them vulnerable to systematic fraud and disinformation.

The challenge of harmonising with international standards is becoming increasingly urgent given the borderless nature of AI, whereby systems developed in other jurisdictions can be accessed and used directly in Indonesia without being subject to local regulatory filters. The European Union has already enacted *the EU AI Act*, which classifies AI based on risk levels and prohibits certain practices deemed to threaten fundamental rights, whilst Singapore has launched a pragmatic and industry-friendly *AI Governance Framework*: (Act, 2024). Indonesia faces a strategic dilemma: adopting strict EU-style standards risks hindering investment flows and technology transfer, yet disregarding global standards could potentially turn Indonesia into *a regulatory haven* for exploitative AI practices rejected in developed nations.

The issues of data sovereignty and infrastructure localisation are also critical points in the regulatory challenges, given that the majority of advanced AI models used in Indonesia are operated by foreign technology companies with servers located outside the national jurisdiction. This dependency poses risks to national security and the leakage of citizens' sensitive data that cannot be accessed by Indonesian law enforcement, a vulnerability that has become increasingly apparent following the enactment of the Personal Data Protection Act (PDP Act) but has not yet been accompanied by adequate implementing regulations regarding cross-border data transfers for AI training purposes (Ministry of Communication and Digital Affairs, 2025). Future regulations must strike a balance between the need for *the free flow of data* to foster innovation and the principle of digital sovereignty, which ensures state control over strategic data assets.

In the context of intellectual property rights (IPR), regulatory uncertainty regarding the ownership status of works generated by generative AI has led to protracted legal disputes between developers, users and the original copyright holders whose works were used to train the models. Indonesian Copyright Law No. 28 of 2014 still requires the element of 'original creation' by 'one or more persons' as the creator, thereby excluding non-human machines from the status of creator and leaving AI-generated works in an ambiguous legal status (Spinello, 2007). This ambiguity not only hinders the commercialisation of AI-based works but also triggers a wave of mass copyright infringements when AI models are trained using datasets that lack clear licensing from rights holders.

Regulatory challenges also extend to labour and social protection, where AI-driven automation has the potential to replace millions of routine jobs without adequate social safety nets and reskilling programmes. Indonesian labour law (Law No. 13 of 2003) and the Law on the National Economic Recovery and Resilience No. 6 of

2023) do not yet specifically address the rights of workers affected by AI disruption, companies' obligations to ensure *a just transition*, or a robot tax as a mechanism for redistributing wealth generated by automation (Plan, 2016) . Failure to regulate these social dimensions could widen economic disparities and trigger social instability, which would ultimately place a burden on the state.

Finally, regulatory challenges are exacerbated by low levels of digital legal literacy among law enforcement officers, judges and prosecutors, who are often technologically illiterate when dealing with complex cases involving algorithmic and digital forensic evidence. The Indonesian judicial system requires specific protocols and intensive training to handle AI disputes, including the establishment of specialised courts or panels of expert judges who understand the technical aspects *of coding*, *data science*, and algorithmic ethics (Alfianto et al., 2024) . Without this institutional capacity-building, even the most sophisticated regulations will be difficult to enforce effectively in court, thereby remaining merely a norm on paper without any real *deterrent effect*.

In summary, the regulatory challenges facing AI in Indonesia are not merely a matter of missing provisions or legislation, but rather a structural crisis involving a skills gap, institutional fragmentation, and a legal paradigm that lags behind in addressing machine autonomy. The necessary legal transformation demands a holistic approach that combines the certainty of *hard law* with the flexibility of *soft law*, as well as close collaboration between policymakers, academics, industry, and civil society. Without radical and adaptive regulatory reform, Indonesia risks falling behind in the global digital economy whilst failing to protect its citizens' fundamental rights from the potential existential dangers of artificial intelligence technology.

Ethics and Data Protection in the Legal Transformation of AI

Legal transformation in the era of artificial intelligence cannot be separated from the ethical dimension, which serves as the moral foundation for the legitimacy of this technology within Indonesia's social order. The key ethical principles that must be adopted within the national AI ecosystem include transparency, fairness, accountability, privacy, and *human agency*, as formulated in the Artificial Intelligence Ethics Guidelines version 1.00 by KORIKA (Firdaus et al., 2026) . However, the implementation of these noble principles in practice faces serious challenges due to a clash with the commercial logic of the technology industry, which often prioritises efficiency and speed of product launch over ethical considerations, thereby creating a wide gap between ideal norms and operational reality.

The most critical ethical issue that has emerged is algorithmic *bias*, which has the potential to perpetuate and even amplify structural discrimination against vulnerable groups on the basis of race, gender, religion and socio-economic status. AI systems learn from historical data that often contains human biases; consequently, when this training data is unrepresentative or biased, the algorithm's output will reproduce such injustices

on a far more massive scale and at a much faster pace (Zeng, 2020) . In diverse Indonesia, instances of this bias can be seen, for example, in banking *credit scoring* systems that systematically reject loan applications from certain regions, or in recruitment algorithms that discriminate against female applicants due to historical data showing male dominance in technical sectors—a reality that contradicts the principle of social justice enshrined in Pancasila.

These ethical challenges are exacerbated by the *'black box'* problem—or the lack of transparency in the decision-making processes of complex AI systems such as *deep learning*—which hinders external audits and public understanding of how decisions that impact their lives are generated. The concept of *Explainable AI* (XAI), which requires that every algorithmic decision be explained in simple human language, has not yet become a mandatory standard in AI development in Indonesia, thereby violating citizens' fundamental right to know the reasons behind administrative or commercial decisions that adversely affect them (Zeng, 2020). Without this transparency, the principle of accountability becomes hollow, as there is no party that can be held morally or legally accountable for system errors.

In the field of personal data protection, the implementation of Law No. 27 of 2022 on Personal Data Protection (PDP Law) within the AI ecosystem faces complex technical dilemmas, particularly regarding the principle *of data minimisation*, which requires data to be collected only to the extent necessary for specific purposes. The characteristics of modern AI, particularly *machine learning* and *generative AI*, actually require massive datasets (*big data*) that often exceed the initial requirements, thereby creating a tension between the technical needs of model training and legal compliance. Recent empirical studies indicate that only 20% of technology start-ups in Indonesia fully adhere to the principle of transparency in data collection for AI, whilst 65% of them do not implement adequate data encryption—a concerning finding amidst the prevalence of data breaches (Rebong et al., 2025) .

The mechanism of *informed consent*, which forms a cornerstone of the Personal Data Protection Act, has also seen its meaning eroded in the context of AI, where users are often faced with lengthy, complex and non-negotiable privacy policies (*take it or leave it*). In many cases, users are unaware that their data is not only processed for immediate services, but is also stored, analysed, and used to train AI models that may be utilised for other commercial purposes in the future—a practice that violates the spirit of individual autonomy (Cohen, 2019) . Worse still, the data subject's right to have their data erased (the 'right *to be* forgotten') becomes almost impossible to implement in AI models that have 'learned' patterns from that data, as removing data from the training dataset does not automatically erase the 'memory' that has been formed within the algorithm's weights.

Threats to privacy are becoming increasingly apparent with the emergence of invasive technologies such as *facial recognition*, biometric tracking and emotion

analysis, which are being increasingly adopted by the public and private sectors in Indonesia without a strong legal basis or independent oversight. The *Indonesia AI Report 2025* reveals that 76% of millennials and 73% of Generation Z are concerned that AI could be used to impersonate them via *deepfake* technology, whilst 65% of respondents are highly protective of their personal data due to fears of misuse (Yu & Zhao, 2019) . These fears are well-founded given the prevalence *of deepfake-based* fraud and the dissemination of non-consensual synthetic content that violates the privacy and dignity of victims; however, law enforcement remains weak due to limitations in digital evidence and investigative capacity.

From a normative ethical perspective, the integration of Pancasila values into AI regulations is essential to ensure that technological transformation does not erode the nation's identity or a just and civilised humanity. The second principle of Pancasila, "Just and Civilised Humanity", demands that AI be developed as a tool to honour humanity, not to degrade its autonomy and dignity through behavioural manipulation or data exploitation(Ma'unah et al., 2025) . However, a review of the literature indicates that AI regulation in Indonesia remains partial and has not yet comprehensively addressed ethical dimensions; consequently, there is a need to formulate an operational, Pancasila-based AI ethics framework that can be tested through algorithmic audits, rather than merely serving as empty rhetoric in strategic documents.

Data protection challenges also include increasingly sophisticated cyber security risks arising from the adoption of AI, where attackers can use *adversarial machine learning* techniques to manipulate data inputs in order to deceive AI systems and steal sensitive information. These AI-based cyberattacks have the potential to cripple critical infrastructure such as banking systems, electricity grids, and healthcare services if not countered with robust security protocols and state-of-the-art encryption standards (Huang et al., 2011). The Personal Data Protection Act (PDP Act) has indeed mandated the obligation of data controllers to secure personal data; however, there are currently no specific technical guidelines regulating AI security standards against adversarial attacks, thereby leaving a vulnerability gap that can be exploited by malicious actors.

Another pressing ethical issue is the use of generative AI to create synthetic content that blurs the line between fact and fiction, triggering an epistemic crisis and eroding public trust in digital information. *Deepfake* technology, capable of producing highly realistic video, audio and text, has been misused for political smear campaigns, financial fraud and virtual sexual harassment; however, Indonesian regulations do not yet include *a mandatory* labelling mechanism for AI-generated content that could help the public distinguish between what is genuine and what is fabricated (Wardle & Derakhshan, 2017). The absence of such standards infringes upon the public's right to accurate information and opens the door to the manipulation of public opinion, which threatens the stability of democracy.

In the context of distributive justice, the legal transformation of AI must also address concerns regarding the widening digital divide, where the economic benefits of AI are enjoyed only by a handful of giant technology companies (*big tech*), whilst the social costs—such as job losses and the erosion of privacy—are borne by the wider public. The principle of justice in AI ethics demands mechanisms for the redistribution of wealth generated by automation, such as *the* proposed robot *tax* or a transitional social security fund, which have so far received little serious attention in national policy discourse (Plan, 2016) . Without pro-equity regulatory intervention, AI has the potential to become a machine of inequality that widens the gap between technology capital owners and the marginalised working class.

The role of independent supervisory bodies, particularly the newly established Personal Data Protection Agency (PDPA), is key to upholding data ethics and protection in the AI era; however, these bodies still face significant challenges in terms of technical capacity, budget and enforcement powers. The Personal Data Protection Act grants the PDPB a broad mandate to develop standards, conduct audits, and impose administrative sanctions; however, its effectiveness will depend heavily on the availability of human resources with expertise in algorithmic forensics and the dynamics of the AI industry(Persadha, 2026) . Without significant institutional strengthening, the PDPB risks becoming a mere 'toothless tiger', unable to stand up to the economic and political power of global technology companies.

The importance of digital ethics literacy and public awareness cannot be overlooked in this legal transformation, as even the strongest regulations will fail without the public's active participation in monitoring and demanding accountability regarding the use of AI. National education programmes need to be expanded to include a basic understanding of how AI works, privacy risks, and citizens' digital rights, so that users are not merely passive objects of data exploitation but active agents capable of protecting themselves and demanding justice (Tumanggor & Sazali, 2025). Pentahelix collaboration between government, academia, industry, the community, and the media is an absolute prerequisite for building an ethical and sovereign AI ecosystem.

In summary, the ethical and data protection challenges in the legal transformation of AI in Indonesia are not merely technical regulatory issues, but a fundamental test of the nation's commitment to human rights, social justice and human dignity in the digital age. The necessary transformation demands a paradigm shift from a *technology-driven* approach that pursues only economic efficiency towards *human-centric AI governance* that places human well-being and the values of Pancasila at the centre of policy. Only with a strong ethical foundation and robust data protection can Indonesia harness the transformative potential of AI without sacrificing its humanity.

Conclusion

Legal transformation in the era of artificial intelligence in Indonesia faces profound structural challenges, characterised by a lack of specific regulations (*a legal vacuum*), fragmentation of authority across institutions, and a legal paradigm that lags behind in responding to algorithmic autonomy. This literature review reveals that the current legal framework, including the ITE Law and the PDP Law, is insufficient to address the complexity of legal liability for discriminatory or fatal AI decisions, particularly due to *the 'black box'* problem which makes it difficult to prove the elements of fault. Without the enactment of specific AI legislation adopting the principle of *strict liability* and mandatory algorithmic audit mechanisms, Indonesia risks facing a serious accountability deficit where victims of technological errors have no effective legal recourse to obtain justice.

Ethical and data protection considerations heighten the urgency of this transformation, where the principles of transparency, fairness and privacy are often eroded by the commercial logic of the technology industry and the limitations of law enforcement capacity. The implementation of the Personal Data Protection Act faces complex technical dilemmas regarding data minimisation, meaningful consent mechanisms, and *the right to erasure* within *machine learning* systems, whilst algorithmic bias risks perpetuating structural discrimination that runs counter to the social justice values of Pancasila. Strengthening the institutional framework of the Personal Data Protection Agency (Badan PDP) and formulating operational AI ethics grounded in Pancasila are absolute prerequisites to ensure that the use of this technology remains humane, sovereign, and just, rather than becoming an instrument of data exploitation and new forms of oppression.

In summary, Indonesia requires a hybrid legal approach that combines the certainty of *hard law* with the flexibility of *soft* law, as well as close pentahelix collaboration between the government, academia, industry, the community and the media. This legal transformation is not merely a technical matter of legislation, but a civilisational project that will determine whether Indonesia is capable of harnessing the transformative potential of AI for Indonesia Emas 2045 without sacrificing human rights, human dignity, and the nation's identity. Urgent strategic recommendations include accelerating the deliberation of the AI Bill, harmonising standards with global frameworks such as *the EU AI Act*, massive investment in digital legal literacy for law enforcement, and the establishment of *a* national *regulatory sandbox* to test innovations within a controlled and ethical environment.

References

Acemoglu, D., & Restrepo, P. (2020). The wrong kind of AI? Artificial intelligence and the future of labour demand. *Cambridge Journal of Regions, Economy and Society*, *13*(1), 25–35.

Act, E. A. I. (2024). The eu artificial intelligence act. *European Union*. https://www.wsgr.com/a/web/qrkz1SnNzWw6nk7B30AyDa/10-things-you-should-know-about-the-eu-artificial-intelligence-act_v2.pdf

Adnin, I., Sapriya, S., Rahmat, R., Ramadhan, A. R., & Juwita, J. (2024). Responsivitas Tenaga Pendidik Terhadap Penyusunan Kebijakan Surat Edaran Pedoman Etika Artificial Intelligence. *PAMARENDA : Public Administration and Government Journal*, *4*(2), 296–302. https://doi.org/10.52423/pamarenda.v4i2.32

Alfianto, D., Rido, A., & Wijaya, G. V. (2024). Pertanggungjawaban Perdata dan Tanggung Gugat Dalam Perkara Wanprestasi Dan Perbuatan Melawan Hukum. *Jurnal Pengabdian Masyarakat: Pemberdayaan, Inovasi Dan Perubahan*, *4*(6). https://doi.org/10.59818/jpm.v4i6.986

Cohen, J. E. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. *Surveillance & Society*, *17*(1/2), 240–245.

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Firdaus, F., Iqbal, M., Sirait, W., Mulyani, L. N., Hidayat, R., & Putri, V. M. (2026). *BUKU AJAR KECERDASAN BUATAN: Panduan Praktis dari Algoritma, Deployment hingga Etika di Era Industri 4.0*. Serasi Media Teknologi.

Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I. P., & Tygar, J. D. (2011). Adversarial machine learning. *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence, AISec '11*, 43–58. https://doi.org/10.1145/2046684.2046692

Indonesia, K. A. (2020). *National Strategy for Artificial Intelligence 2020-2045 (2020)(Indonesian)*. https://openresearch-repository.anu.edu.au/bitstreams/a954ab22-5b81-45de-80ed-823deffe3820/download

Li, Y., Shao, S., He, Y., Guo, J., Zhang, T., Qin, Z., Chen, P.-Y., Backes, M., Torr, P., Tao, D., & Ren, K. (2025). *Rethinking Data Protection in the (Generative) Artificial Intelligence Era* (arXiv:2507.03034). arXiv. https://doi.org/10.48550/arXiv.2507.03034

Ma'unah, I., Musyarofah, S., Zahra, A. F. Z. A., & Agrariyanti, Y. (2025). Pancasila dan Artificial Intelligence: Analisis Etis atas Regulasi AI di Indonesia: Pancasila and Artificial Intelligence: Ethical Analysis of AI Regulations in Indonesia. *LITERA: Jurnal Ilmiah Mutidisiplin*, *2*(5), 718–746.

Persadha, D. P. (2026). *BADAN PDP DAN MASA DEPAN KEDAULATAN DIGITAL INDONESIA*. CISSREC.

Plan, S. (2016). The national artificial intelligence research and development strategic plan. *National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee*. http://large.stanford.edu/courses/2018/ph241/cheng1/docs/ai-eop-oct16.pdf

Pradana, A. E., Herawati, A. R., Dwimawanti, I. H., & Maesaroh. (2025). Tantangan Kecerdasan Buatan Dalam Implikasi Kebijakan Pemerintah di Indonesia: Studi Literatur. *Jurnal Good Governance*, 51–66. https://doi.org/10.32834/gg.v21i1.889

Purbasari, R., Munajat, E., Fauzan, F., & Hakim, M. A. (2025). Model of Digital Collaboration Network in Digital Innovation Context: Social Network Analysis Approach. *Review of Integrative Business and Economics Research*, *14*(1), 614–633.

Ravizki, E. N., & Yudhantaka, L. (2022). Artificial Intelligence Sebagai Subjek Hukum: Tinjauan Konseptual dan Tantangan Pengaturan di Indonesia. *Notaire*, *5*(3). https://e-journal.unair.ac.id/NTR/article/download/39063/22918

Rebong, T. G. D., Hambali, J. H., & Timothy, F. (2025). Implementasi UU PDP Indonesia Dalam Pengembangan Sistem Kecerdasan Buatan: Tantangan dan Peluang. *Cerdika: Jurnal Ilmiah Indonesia*, *5*(10), 2274. https://doi.org/10.59141/cerdika.v5i10.2856

Respati, A. A. (2024). Reformulasi UU ITE terhadap Artificial Intelligence Dibandingkan dengan Uni Eropa dan China AI Act Regulation. *JURNAL USM LAW REVIEW*, *7*(3), 1737–1758. https://doi.org/10.26623/julr.v7i3.10578

Ridhwan, M. M. (2025). *The Impact of E-Commerce Adoption on Micro, Small, and Medium Enterprises Performance in Rural Areas: Evidence from Indonesia* (SSRN Scholarly Paper No. 5581690). Social Science Research Network. https://doi.org/10.2139/ssrn.5581690

Spinello, R. A. (2007). Intellectual property rights. *Library Hi Tech*, *25*(1), 12–22. https://doi.org/10.1108/07378830710735821

Sukmaningsih, N. K. I. A. (2025). Urgensi Pengaturan Hak Cipta di Era Kecerdasan Buatan: Tantangan dan Solusi Hukum di Indonesia. *Prosiding Seminar Nasional Hukum, Bisnis, Sains Dan Teknologi*, *5*(1), 16–22.

Sulistio, F., & Salsabilla, A. D. (2023). Pertanggungjawaban pada Tindak Pidana yang Dilakukan Agen Otonom Artificial Intelegence. *UNES Law Review*, *6*(2), 5479–5490. https://doi.org/10.31933/unesrev.v6i2.1209

Tumanggor, T., & Sazali, H. (2025). Etika Regulasi dan Kebijakan Media Digital: Meningkatkan Kesadaran Publik di Era Informasi. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi*, *6*(3), 1657–1669. https://doi.org/10.63447/jimik.v6i3.1565

Valdivia, A. N. (2018). Algorithms of Oppression: How Search Engines Reinforce Racism by Safiya Umoja Noble (review). *Feminist Formations*, *30*(3), 217–220.

Walliman, N., & Walliman, N. (2021). *Research Methods: The Basics* (3rd ed.). Routledge. https://doi.org/10.4324/9781003141693

Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policymaking* (Vol. 27). Council of Europe Strasbourg. https://www.firstdraftnews.org/wp-content/uploads/2017/11/PREMS-162317-GBR-2018-Report-de%CC%81sinformation-1.pdf

Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, *35*(5), 105318. https://doi.org/10.1016/j.clsr.2019.04.001

Yuliana, S., & Anita, D. (2026). Pelayanan Publik Digital sebagai Instrumen Peningkatan Kepercayaan Masyarakat terhadap Pemerintah. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *4*(4), 13973–13980. https://doi.org/10.31004/riggs.v4i4.5407

Zeng, J. (2020). Artificial intelligence and China's authoritarian governance. *International Affairs*, *96*(6), 1441–1459. https://doi.org/10.1093/ia/iiaa172

Pemerintah Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 197.