A Legal Perspective on the Use of Large Language Models in the Era of Artificial Intelligence

Y Zahra
Faculty of law, Sriwijaya University, Palembang, Indonesia

Article Info

Article history:

Received Feb 8th, 2026
Revised Feb 19th, 2026
Accepted Feb 23th, 2026

Corresponding Author:

Y Zahra
Email: sansen321@gmail.com
Indonesia

Abstract

This study examines the legal implications of Large Language Models (LLMs) within the Indonesian regulatory framework. As AI technologies rapidly evolve, Indonesia relies primarily on general laws on data protection, electronic systems, civil liability, and intellectual property to govern AI deployment. However, these laws were not specifically designed to address the autonomous and generative nature of LLMs. This research employs a normative legal methodology to analyze statutory provisions, identify regulatory gaps, and evaluate constitutional principles relevant to AI governance. The findings reveal fragmentation, ambiguity in training data legality, uncertainty in liability allocation, and limited transparency requirements. The study proposes a risk based and accountability-oriented governance framework that harmonizes existing sectoral regulations while strengthening human rights protection. By developing a coherent regulatory approach, Indonesia can enhance legal certainty, mitigate technological risks, and promote responsible innovation in the era of artificial intelligence.

Keywords *Large Language Models; AI Governance; Indonesian Law*

Abstrak

Penelitian ini mengkaji implikasi hukum penggunaan Large Language Models (LLMs) dalam kerangka regulasi Indonesia. Seiring pesatnya perkembangan teknologi kecerdasan buatan, Indonesia masih mengandalkan regulasi umum seperti perlindungan data pribadi, sistem elektronik, tanggung jawab perdata, dan hak kekayaan intelektual untuk mengatur implementasi AI. Namun, regulasi tersebut belum secara spesifik dirancang untuk menghadapi karakteristik otonom dan generatif LLM. Penelitian ini menggunakan metode hukum normatif untuk menganalisis ketentuan peraturan perundang-undangan, mengidentifikasi kesenjangan regulasi, serta mengevaluasi prinsip konstitusional yang relevan dengan tata kelola AI. Hasil penelitian menunjukkan adanya fragmentasi regulasi, ambiguitas legalitas data pelatihan, ketidakjelasan alokasi tanggung jawab, serta keterbatasan kewajiban transparansi. Penelitian ini mengusulkan kerangka tata kelola berbasis risiko dan akuntabilitas guna memperkuat kepastian hukum, perlindungan hak asasi manusia, dan inovasi yang bertanggung jawab.

Kata kunci: Large Language Models; Tata Kelola AI; Hukum Indonesia

1. INTRODUCTION

The rapid advancement of artificial intelligence (AI) technologies has significantly transformed the digital landscape, reshaping how information is created, processed, and distributed. Among the most transformative developments are Large Language Models (LLMs), which are capable of generating human like text, analyzing complex data patterns, and supporting decision-making across various sectors [1]-[5].

From education and business to public administration and legal services, LLMs are increasingly integrated into everyday digital infrastructures. While these systems offer remarkable opportunities for innovation and efficiency, they also introduce complex legal and regulatory challenges that demand careful examination.

In Indonesia, the growth of AI technologies has accelerated alongside digital transformation initiatives and national strategies promoting technological innovation. However, the legal system has not evolved at the same pace as technological development. Existing regulatory frameworks primarily those governing data protection, electronic systems, and intellectual property were designed for conventional digital platforms rather than autonomous, generative AI systems. As a result, important questions arise concerning the adequacy of current laws in addressing the unique characteristics of LLMs. One of the central legal concerns involves the processing of vast quantities of data used to train LLMs. These systems rely on large-scale datasets, often including publicly accessible digital content, raising questions about consent, lawful processing, and the boundaries of legitimate data use [6]-[8]. Additionally, the probabilistic nature of LLM outputs challenges traditional doctrines of liability and accountability, particularly when harmful, misleading, or biased content is generated. Determining who bears legal responsibility the developer, deployer, or user remains a complex and unresolved issue within the Indonesian legal context.

Beyond privacy and liability, intellectual property rights present another layer of legal uncertainty [9],[10]. Indonesian copyright law emphasizes human authorship and creative expression, which creates ambiguity regarding the ownership and protection of AI generated works. Furthermore, the potential for algorithmic bias and discriminatory outcomes raises constitutional concerns related to equality before the law and the protection of fundamental rights. Without appropriate safeguards, the deployment of LLMs may inadvertently undermine principles enshrined in Indonesia's constitutional framework. These challenges illustrate a broader phenomenon often described as regulatory lag, where technological innovation advances more rapidly than legislative reform [11]-[15]. In such circumstances, the law risks becoming reactive rather than proactive. For Indonesia, this regulatory gap may create uncertainty for AI developers, businesses, and public institutions, while also exposing individuals to potential rights violations. A coherent legal framework that balances innovation with accountability is therefore essential.

This study seeks to provide a comprehensive legal analysis of the use of Large Language Models within the Indonesian context. By examining existing laws, identifying normative gaps, and evaluating constitutional principles, the research aims to develop a structured governance framework that ensures legal certainty, accountability, and human rights protection. Ultimately, the study contributes to the broader discourse on AI governance by proposing a balanced regulatory approach that supports responsible innovation while safeguarding fundamental legal values in the era of artificial intelligence.

2. METHOD

This study employs a normative legal research methodology to critically examine the use of Large Language Models (LLMs) within the broader framework of artificial intelligence governance (Figure 1). The research begins with the identification of core legal problems related to the use of Large Language Models (LLMs) in the contemporary artificial intelligence landscape. At this stage, the study defines the primary legal concerns, such as data protection, civil and criminal liability, intellectual property rights, algorithmic bias, transparency, and accountability. This step establishes the conceptual boundaries of the research and ensures that the analysis remains focused on legally relevant and normatively significant issues. Following the identification of the legal problems, the study formulates clear research objectives and research questions. These objectives aim to evaluate the adequacy, coherence, and effectiveness of existing legal frameworks governing LLMs. The research questions are structured to explore whether current regulations sufficiently address technological risks, whether normative gaps exist, and how legal governance can be improved. The scope of the research is also defined in terms of jurisdictional coverage and regulatory focus.

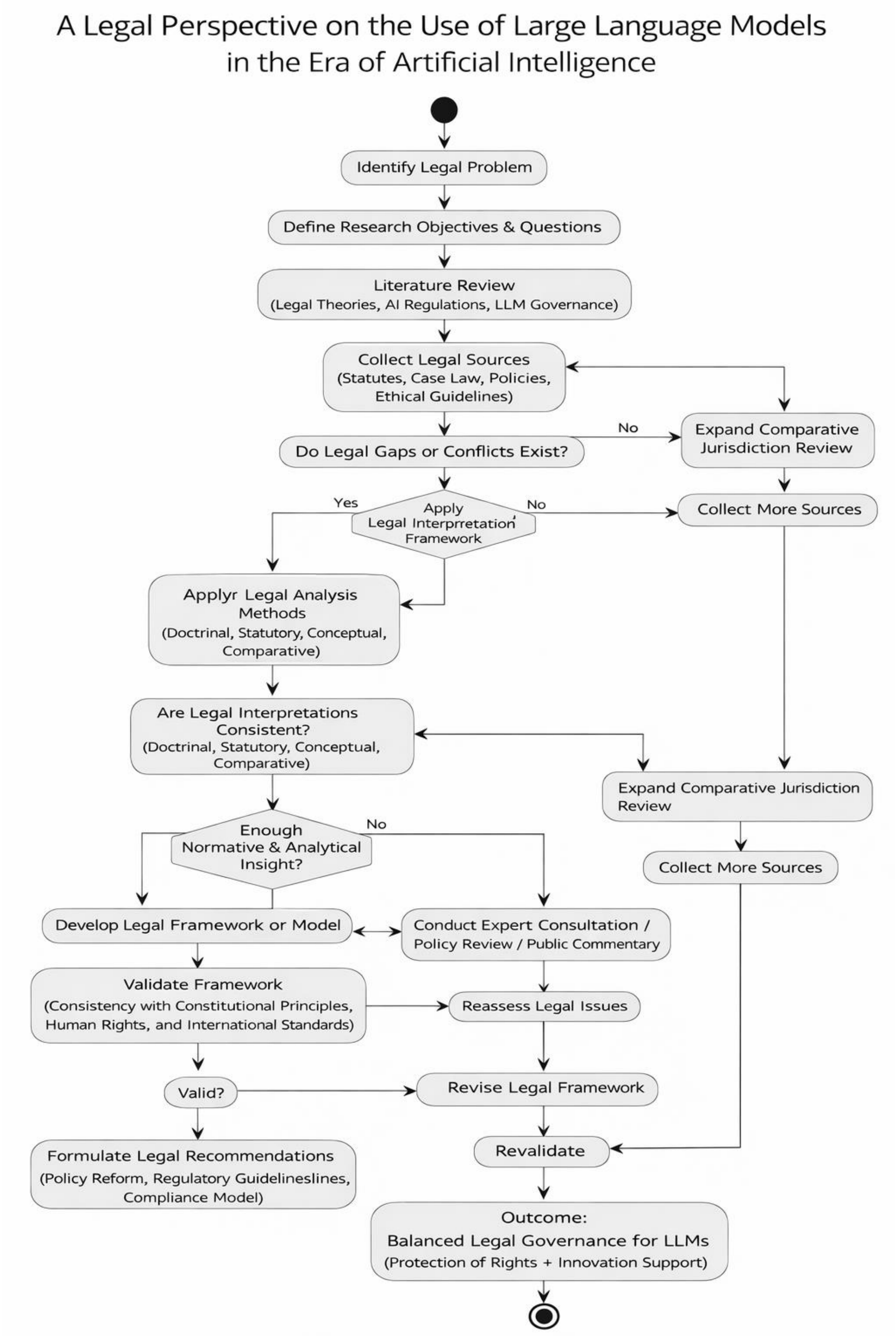
A Legal Perspective on the Use of Large Language Models in the Era of Artificial Intelligence
Identify Legal Problem
Define Research Objectives & Questions
Literature Review (Legal Theories, AI Regulations, LLM Governance)
Collect Legal Sources (Statutes, Case Law, Policies, Ethical Guidelines)
Do Legal Gaps or Conflicts Exist?
No
Expand Comparative Jurisdiction Review
Yes
Apply Legal Interprretation Framework
No
Collect More Sources
Applyr Legal Analysis Methods (Doctrinal, Statutory, Conceptual, Comparative)
Are Legal Interpretations Consistent? (Doctrinal, Statutory, Conceptual, Comparative)
Expand Comparative Jurisdiction Review
Collect More Sources
Enough Normative & Analytical Insight?
No
Develop Legal Framework or Model
Conduct Expert Consultation / Policy Review / Public Commentary
Validate Framework (Consistency with Constitutional Principles, Human Rights, and International Standards)
Reassess Legal Issues
Valid?
Revise Legal Framework
Revalidate
Formulate Legal Recommendations (Policy Reform, Regulatory Guidelineslines, Compliance Model)
Outcome: Balanced Legal Governance for LLMs (Protection of Rights + Innovation Support)

Figure 1 – Legal methodology for AI governance

The next stage involves a comprehensive literature review. This includes an examination of legal theory, constitutional principles, regulatory theory, AI governance scholarship, and interdisciplinary academic discussions concerning emerging technologies. The purpose of this review is to construct a strong theoretical foundation and to situate the study within existing academic debates on technology regulation and digital governance. Subsequently, the research collects and classifies legal sources, which are categorized as follows (Table 1):

Table 1 – Legal sources classification

Type of Source	Examples	Function
Primary Legal Sources	Statutes, AI regulations, court decisions	Normative foundation
Secondary Legal Sources	Books, journal articles, policy papers	Interpretation and analysis
Tertiary Legal Sources	Legal encyclopedias, international reports	Conceptual reinforcement

After gathering the legal materials, the study proceeds to identify potential legal gaps or normative conflicts. This stage assesses whether regulatory vacuums exist, whether overlapping or contradictory norms are present, and whether existing laws are inadequate to address the technical characteristics of LLMs. If no substantial gap is identified, the research expands into comparative jurisdictional review to ensure analytical depth. If gaps or inconsistencies are found, the study advances to a more detailed doctrinal analysis. The research then applies multiple legal analytical approaches to examine the issues comprehensively (Table 2):

Table 2 – Multiple legal analytical approaches

Approach	Analytical Focus	Purpose
Doctrinal	Interpretation of written norms	Assess legal consistency
Statutory	Examination of legislation	Evaluate regulatory adequacy
Conceptual	Analysis of legal concepts	Clarify principles and terminology
Comparative	Cross-jurisdiction comparison	Identify best practices

Through these approaches, the study evaluates whether legal interpretations are coherent and consistent with constitutional principles, rule of law standards, and human rights norms. Where inconsistencies arise, the interpretative framework is refined and reassessed. The analysis then concentrates on key substantive legal issues associated with LLM deployment (Table 3):

Table 3 – Legal issues associated with LLM deployment

Issue	Critical Question
Privacy	Does training data processing violate data protection laws?
Liability	Who is responsible for harmful LLM outputs?
Intellectual Property	Do generated outputs infringe copyright?
Bias	Do LLM systems produce discriminatory outcomes?
Accountability	How can responsibility and oversight be ensured?

If the normative and analytical insights remain insufficient, the study incorporates expert consultations, policy analysis, regulatory commentaries, and broader socio legal considerations. This step ensures that the legal analysis reflects practical realities and regulatory developments. Based on the accumulated findings, the research develops a structured legal framework or governance model for LLMs. This model outlines regulatory principles, compliance mechanisms, supervisory structures, and allocation of legal responsibility. The framework is designed to align with constitutional values, proportionality principles, human rights protections, and international AI governance standards. The proposed framework is subsequently validated by assessing its internal coherence, constitutional compatibility, and consistency with international legal norms. If deficiencies are identified, revisions are undertaken and the model is revalidated.

Finally, the study formulates legal and policy recommendations. These include proposals for regulatory reform, compliance guidelines for AI developers and deployers, accountability mechanisms, and strategies for harmonizing domestic regulations with international standards. The ultimate outcome of the methodology is the development of a balanced legal governance model for Large Language Models one that simultaneously safeguards fundamental rights, ensures legal certainty, mitigates technological risks, and supports responsible innovation in the era of artificial intelligence.

3. RESULT AND DISCUSSION

The findings indicate that Indonesia does not yet have a comprehensive and AI-specific regulatory framework governing the development and deployment of Large Language Models (LLMs). Instead, regulatory oversight is fragmented across several sectoral laws, which indirectly apply to AI technologies. From a data protection perspective, the enactment of Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (Personal Data Protection Law or PDP Law) provides a foundational framework for lawful data processing. However, the study finds significant ambiguity regarding the legality of large-scale data scraping for AI training, the definition of "publicly available data," and the applicability of consent requirements in machine learning contexts. The absence of implementing regulations specifically addressing AI training practices creates interpretative uncertainty.

In the area of electronic systems governance, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE Law) and its implementing regulation, Peraturan Pemerintah Nomor 71 Tahun 2019, impose obligations on Electronic System Operators (PSE), including reliability, security, and accountability standards. Nevertheless, these provisions were designed for conventional digital platforms and do not explicitly regulate autonomous AI decision making systems or generative models. With regard to intellectual property, Undang-Undang Nomor 28 Tahun 2014 tentang Hak Cipta (Copyright Law) protects human created works but does not clearly address authorship and ownership of AI generated outputs. The law's emphasis on human creativity raises interpretative challenges when LLM generated content lacks direct human authorship.

Concerning liability, Indonesia relies on general civil law principles under the Civil Code (KUHPerdata), particularly unlawful acts (perbuatan melawan hukum). However, the study finds that attributing liability within an AI ecosystem where developers, deployers, and users interact remains legally uncertain. No specific statutory provision currently allocates strict or shared liability for AI generated harm. Additionally, the constitutional dimension is significant. Undang-Undang Dasar Negara Republik Indonesia Tahun 1945 (1945 Constitution) guarantees the right to privacy, legal certainty, and equal protection before the law. The absence of AI specific safeguards may create risks of constitutional rights violations, particularly in cases involving automated profiling or discriminatory outputs. The key findings are summarized below (Table 4):

Table 4 – The key findings

Legal Area	Existing Indonesian Regulation	Identified Gap	Risk Level
Data Protection	UU PDP 2022	Unclear rules on AI training data & automated processing	High
Electronic Systems	UU ITE & PP 71/2019	No explicit AI governance provisions	High
Intellectual Property	UU Hak Cipta 2014	No recognition of AI-generated works	Medium–High
Civil Liability	Civil Code (PMH doctrine)	Unclear liability allocation in AI ecosystem	High
Constitutional Rights	UUD 1945	Lack of AI-specific rights safeguards	High

Overall, the results demonstrate that Indonesia's legal framework provides general digital governance mechanisms but lacks a dedicated and coherent AI regulatory regime. The discussion reveals that

Indonesia is currently in a transitional regulatory phase regarding AI governance. Existing laws are technology-neutral and principle based, which allows some flexibility but also creates interpretative gaps when applied to complex LLM systems. A major issue is regulatory fragmentation. The PDP Law emphasizes personal data protection, while the ITE Law focuses on electronic system reliability. However, neither statute comprehensively addresses algorithmic transparency, automated decision-making accountability, or systemic AI risk management. This fragmentation may lead to inconsistent enforcement across institutions, including the Ministry of Communication and Digital Affairs (Kominfo) and sectoral regulators.

Another critical issue concerns the legality of data scraping practices. Under the PDP Law, lawful processing requires a valid legal basis such as consent or legitimate interest. However, the law does not explicitly clarify whether publicly accessible online data may be freely used for AI training without individual consent. This ambiguity poses compliance risks for domestic AI developers and foreign AI providers operating in Indonesia. In terms of liability, reliance on the unlawful act doctrine (perbuatan melawan hukum) may be insufficient for AI related harm, as it requires proof of fault, causation, and damage. Given the probabilistic and non deterministic nature of LLM outputs, establishing causation could be legally complex. Therefore, the discussion suggests the potential need for a modified liability regime such as shared liability or risk-based responsibility allocation. The study also identifies a constitutional imperative to ensure that AI deployment does not undermine equality before the law and non-discrimination principles. Bias in LLM outputs, particularly in employment, financial services, or public administration contexts, could raise constitutional challenges if not properly regulated. A proposed Indonesian governance model for LLMs may follow this layered structure (Figure 2):

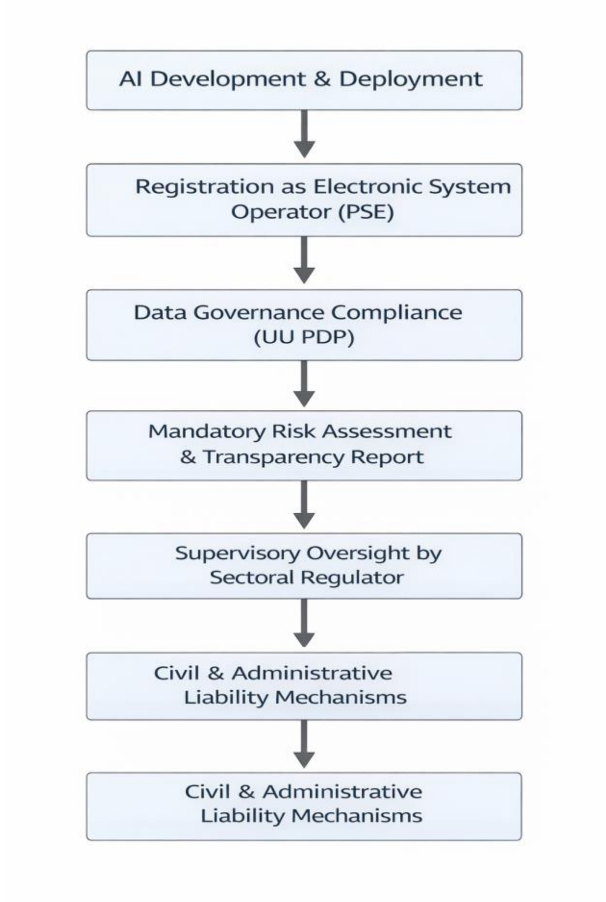
AI Development & Deployment
Registration as Electronic System Operator (PSE)
Data Governance Compliance (UU PDP)
Mandatory Risk Assessment & Transparency Report
Supervisory Oversight by Sectoral Regulator
Civil & Administrative Liability Mechanisms
Civil & Administrative Liability Mechanisms

Figure 2 – A proposed Indonesian governance model for LLMs

This model integrates existing regulatory instruments while introducing AI specific compliance mechanisms such as algorithmic impact assessments, bias audits, and transparency reporting obligations. The normative implications for Indonesia are summarized below (Table 5):

Table 5 – The normative implications

Governance Principle	Regulatory Implication in Indonesia
Legal Certainty	Issuance of AI specific implementing regulations
Accountability	Clear allocation of developer and deployer liability
Transparency	Mandatory AI system documentation & reporting
Proportionality	Risk based obligations depending on AI application
Human Rights Protection	Alignment with constitutional guarantees

The Indonesian legal system possesses a foundational regulatory structure capable of supporting AI governance. However, without explicit AI focused legislation or implementing regulations, significant legal uncertainty persists. To ensure balanced governance, Indonesia should adopt a coherent AI regulatory framework that harmonizes the PDP Law, ITE Law, intellectual property law, and constitutional principles. Such reform would enhance legal certainty, protect fundamental rights, and promote responsible innovation in the era of Large Language Models.

4. CONCLUSION

The regulation of Large Language Models in Indonesia remains at a formative stage, relying largely on general digital, data protection, and civil liability frameworks that were not specifically designed for advanced AI systems. While existing laws such as the Personal Data Protection Law and the Electronic Information and Transactions Law provide an important legal foundation, they do not yet offer comprehensive guidance on issues such as AI training data, algorithmic transparency, and responsibility allocation. This regulatory gap creates both legal uncertainty and potential risks to constitutional rights, including privacy and equality before the law. Moving forward, Indonesia would benefit from a coherent, risk-based AI governance framework that strengthens accountability, ensures transparency, and harmonizes sectoral regulations. By adopting a balanced and forward-looking approach, Indonesia can protect fundamental rights while still encouraging innovation and responsible technological development in the era of artificial intelligence.

REFERENCES

[1] P. B. Alla, “Augmenting Intelligent Process Automation through Generative AI for Human-in-the-Loop Decision Systems,” *Digit. Eng.*, vol. 8, no. November 2025, p. 100071, 2026, doi: https://doi.org/10.1016/j.dte.2025.100071.

[2] K. Y. Lim and R. Darvin, “Critical digital literacies , generative AI , and the negotiation of agency in human-AI interactions,” *System*, vol. 136, no. April 2025, p. 103904, 2026, doi: https://doi.org/10.1016/j.system.2025.103904.

[3] M. Tedre and H. Vartiainen, “Emerging human-technology relationships in a co-design process with generative AI,” vol. 56, no. November 2024, 2025, doi: https://doi.org/10.1016/j.tsc.2024.101742.

[4] R. Mohawesh, M. Ashraf, and H. Bany, “A data-driven risk assessment of cybersecurity challenges posed by generative AI,” *Decis. Anal. J.*, vol. 15, no. March, p. 100580, 2025, doi: https://doi.org/10.1016/j.dajour.2025.100580.

[5] A. Matharaarachchi and H. Moraliyage, “Knowledge-Based Systems Addressing hallucinations in generative AI agents using observability and dual memory knowledge graphs,” *Knowledge-Based Syst.*, vol. 338, no. February, p. 115469, 2026, doi: https://doi.org/10.1016/j.knosys.2026.115469.

[6] F. Romero-moreno, *Computer Law & Security Review : The International Journal of Technology Law and Practice Deepfake detection in generative AI : A legal framework proposal to protect human rights*, vol. 58, no. June. Elsevier Ltd, 2025. doi: https://doi.org/10.1016/j.clsr.2025.106162.

[7] X. Ye and Y. Yan, “Privacy and personal data risk governance for generative artificial intelligence : A Chinese perspective,” *Telecomm. Policy*, vol. 48, no. 10, p. 102851, 2024, doi: https://doi.org/10.1016/j.telpol.2024.102851.

[8] A. Cordella and F. Gualdi, “Regulating generative AI : The limits of technology-neutral regulatory frameworks . Insights from Italy ’ s intervention on ChatGPT,” *Gov. Inf. Q.*, vol. 41, no. 4, p. 101982, 2024, doi: https://doi.org/10.1016/j.giq.2024.101982.

[9] H. M. Khawand, M. Kittler, D. Mortelmans, and U. Chrisitan, “Intellectual property and exit strategies among SMEs : A scoping review and framework,” *World Pat. Inf.*, vol. 79, no. October, p. 102318, 2024, doi: https://doi.org/10.1016/j.wpi.2024.102318.

[10] E. Elmahjub, “Computer Law & Security Review : The International Journal of Technology Law and Practice The algorithmic muse and the public domain : Why copyright ’ s legal philosophy precludes protection for generative AI outputs,” *Comput. Law Secur. Rev. Int. J. Technol. Law Pract.*, vol. 58, no. July, p. 106170, 2025, doi: https://doi.org/10.1016/j.clsr.2025.106170.

[11] O. A. Shonubi, “Innovation challenges of digital transformation : Transitioning legacy to the future,” vol. 10, no. September 2024, 2025.

[12] J. Woo and K. Lee, “Building a consensus : Harmonizing AI ethical guidelines and legal frameworks in Korea for enhanced

governance," *Gov. Inf. Q.*, vol. 42, no. 3, p. 102060, 2025, doi: https://doi.org/10.1016/j.giq.2025.102060.

[13] H. Zahid, A. Zulfiqar, M. Adnan, and S. Iqbal, "Results in Engineering Review article A review on socio-technical transition pathway to European super smart grid : Trends , challenges and way forward via enabling technologies," *Results Eng.*, vol. 25, no. November 2024, p. 104155, 2025, doi: https://doi.org/10.1016/j.rineng.2025.104155.

[14] N. Hynek, B. Gavurova, and M. Kubak, "Risks and benefits of artificial intelligence deepfakes : Systematic review and comparison of public attitudes in seven European Countries," *J. Innov. Knowl.*, vol. 10, no. 5, p. 100782, 2025, doi: https://doi.org/10.1016/j.jik.2025.100782.

[15] P. Quintais, "Computer Law & Security Review : The International Journal of Technology Law and Practice Generative AI , copyright and the AI Act," vol. 56, no. January, 2025, doi: https://doi.org/10.1016/j.clsr.2025.106107.