Legal Autonomous Web-based Governance (LAW)
Vol. 1, No. 2, October 2026, pp. 242∼253
E-ISSN: 3164-6794 | P-ISSN: 3164-6697, DOI: 10.68012

Human Rights Centered AI Governance for Emerging Economies

Marviola Hardini[1], Richard Andre Sunarjo[2], Nyree Ani[3*], Apriani Sijabat[4]
[1,2]Faculty of Economics and Business, Universitas Raharja, Indonesia
[3]Department of Cyber Law and Digital Rights, Pandawan Incorporation, New Zealand
[4]Faculty of Teacher Training and Education, University of HKBP Nommensen Pematangsiantar, Indonesia
[1]marviola@raharja.info, [2]richard.sunarjo@raharja.info, [3]nyreeani@pandawan.ac.nz, [4]aprianisijabat@gmail.com
***Corresponding Author**

Article Info

Article history:

Submission April 23, 2026
Revised September 21, 2026
Accepted September 28, 2026
Published September 30, 2026

Keywords:

Artificial Intelligence
AI Regulation
Digital Human Rights
Emerging Economies
AI Governance

ABSTRACT

Artificial Intelligence (AI) is increasingly deployed in socially significant domains, creating regulatory challenges concerning privacy, equality, non-discrimination, transparency, accountability, and access to effective remedies, particularly in emerging economies. **This study examines** how AI regulation can protect digital human rights while supporting technological innovation and inclusive digital development. **The study employs** normative legal research combined with comparative legal analysis of international instruments, selected national and regional regulatory frameworks, human-rights instruments, data protection regulations, academic literature, and institutional reports. **The analysis finds that** AI governance is shifting from voluntary ethical principles toward rights-based and risk-oriented regulation, but significant implementation gaps remain because of differences in institutional capacity, regulatory maturity, technological infrastructure, technical expertise, and enforcement mechanisms. Based on these findings, the study proposes a human-rights-centered AI governance framework built around four interconnected pillars that encompass rights protection, risk governance, institutional accountability and regulatory adaptability. The framework extends existing AI governance approaches by connecting substantive human-rights protection with preventive risk management, clearly allocated institutional responsibilities, and context-sensitive regulatory adaptation for emerging economies. **The study concludes** that effective AI regulation should be assessed by its capacity to provide meaningful, enforceable, and accessible protection of digital human rights throughout the AI lifecycle while enabling responsible innovation and inclusive socioeconomic development.

This is an open access article under the CC BY 4.0 license.

DOI: https://doi.org/10.68012/law.v1i2.173
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)
©Authors retain all copyrights

1. INTRODUCTION

Artificial Intelligence (AI) has become increasingly integrated into public administration, finance, healthcare, education, employment, law enforcement, and digital platforms [1]. These applications offer opportunities to improve efficiency, decision-making, and socioeconomic development. However, the growing use of AI also creates significant challenges for human rights, particularly regarding privacy, equality, non-discrimination, transparency, accountability, and access to effective remedies [2]. As AI systems increasingly

influence decisions affecting individuals and communities, regulatory frameworks must ensure that technological development remains consistent with human dignity and fundamental rights [3].

These challenges are particularly complex in emerging economies, where regulatory maturity, institutional capacity, technical expertise, digital infrastructure, and enforcement resources vary considerably [4]. Limited capacity to conduct algorithmic assessments, monitor AI systems, protect personal data, and enforce regulatory requirements may increase the vulnerability of individuals and marginalized groups [5]. At the same time, differences in regulatory capacity between domestic institutions and multinational technology companies can create additional difficulties in ensuring effective accountability and rights protection [6].

Although international organizations have developed principles and frameworks for responsible AI, translating these principles into enforceable legal and institutional mechanisms remains challenging [7]. Existing approaches often emphasize individual aspects of AI governance, such as ethical principles, risk management, data protection, or transparency. However, these approaches may not fully address the interconnected requirements of human rights protection, institutional accountability, and regulatory implementation in emerging-economy contexts [8]. This creates a need for a regulatory framework that connects normative human rights principles with practical mechanisms for risk management, oversight, and enforcement.

Therefore, this study examines how AI regulation can protect digital human rights in emerging economies while supporting responsible innovation and inclusive socioeconomic development [9]. The analysis focuses on seven regulatory dimensions: privacy and data protection, equality and non-discrimination, transparency and explainability, human oversight, accountability, risk assessment and management, and access to remedies and redress. These dimensions are examined through normative legal research and comparative legal analysis of international instruments, selected regulatory frameworks, human rights instruments, data protection regulations, academic literature, and institutional reports [10].

This study contributes to a human-rights-centered AI governance framework structured around four interconnected pillars: rights protection, risk governance, institutional accountability, and regulatory adaptability. The framework aims to connect rights-based principles with practical regulatory mechanisms that can be adapted to the institutional and regulatory conditions of emerging economies. Accordingly, the study addresses the following research question:

- How can AI regulation protect digital human rights in emerging economies while supporting responsible innovation and inclusive development?

The proposed framework contributes to SDG 16 through institutional accountability and access to remedies, SDG 10 through protection against algorithmic discrimination and unequal risks, and SDG 9 through responsible technological innovation and regulatory adaptability.

2. LITERATURE REVIEW

2.1. AI Regulation and Digital Human Rights

AI regulation has evolved from voluntary ethical principles toward more structured and risk-oriented governance frameworks [11]. International frameworks increasingly emphasize transparency, fairness, privacy, human oversight, accountability, and risk management across the AI lifecycle. This development reflects a growing recognition that AI governance should not focus solely on technological performance but also on its potential effects on fundamental rights and social well-being [12].

Digital human rights provide an important normative foundation for AI regulation. The application of AI to decisions affecting individuals raises concerns regarding privacy, autonomy, equality, non-discrimination, freedom, and access to effective remedies [13]. In particular, algorithmic decision-making may reproduce or amplify existing forms of discrimination, while opaque systems can make it difficult for affected individuals to understand or challenge decisions. Consequently, transparency, explainability, human oversight, and accountability have become important elements of rights-oriented AI governance [14].

Recent literature also indicates a convergence between human-rights-based and risk-based approaches. Human rights establish the principles that should be protected, while risk-based governance provides mechanisms for identifying, assessing, and mitigating potential harms [15]. Institutional accountability complements both approaches by establishing responsibilities for organizations, regulators, and other relevant actors.

2.2. AI Risks and Challenges in Emerging Economies

The implementation of AI governance presents additional challenges in emerging economies. Differences in regulatory maturity, institutional capacity, technical expertise, digital infrastructure, and enforcement resources can limit the practical implementation of AI governance principles [16]. Although international frameworks provide common normative directions, their application may vary significantly according to national legal and institutional conditions [17]. AI-related risks in these contexts include privacy violations, algorithmic discrimination, limited transparency, inadequate human oversight, weak accountability, and difficulties in accessing remedies. These challenges may be more significant where regulatory institutions lack sufficient technical expertise or resources to conduct assessments, monitor AI systems, and enforce compliance [18]. Therefore, effective AI governance requires not only formal regulatory provisions but also institutional mechanisms capable of implementing and adapting them to local conditions [19].

2.3. Research Gap

Existing studies have extensively examined AI ethics, risk-based regulation, digital human rights, data protection, and institutional accountability [20]. However, these perspectives are often addressed separately, while their integration within the specific institutional conditions of emerging economies remains less developed [21]. The main gap therefore concerns how human-rights principles can be translated into practical and enforceable regulatory mechanisms while accounting for differences in institutional capacity and regulatory maturity [22]. To address this gap, this study integrates eight regulatory dimensions—privacy and data protection, equality and non-discrimination, transparency and explainability, human oversight, accountability, risk assessment and management, and access to remedies—into four interconnected pillars: rights protection, risk governance, institutional accountability, and regulatory adaptability. This framework provides a basis for examining AI governance from both a human-rights and implementation perspective in emerging economies [23].

Table 1. Synthesis of Recent Studies on AI Regulation and Digital Human Rights

Approach	Main Focus	Limitation
Human-rights-based	Rights, dignity, equality	Limited operational mechanisms
Risk-based	Risk identification and mitigation	May not ensure remedies
Institutional	Accountability and oversight	Depends on institutional capacity

Table 1 summarizes three complementary approaches to AI regulation: human-rights-based governance, risk-based governance, and institutional accountability. These approaches provide the foundation for integrating rights protection, risk management, and regulatory oversight into a human-rights-centered AI governance framework for emerging economies.

3. RESEARCH METHOD

3.1. Research Design and Approach

This study employs a normative legal research approach combined with comparative legal analysis to examine the relationship between AI regulation and the protection of digital human rights in emerging economies [24]. The normative approach is selected because the research primarily investigates legal norms, regulatory principles, institutional responsibilities, and governance mechanisms governing the development and deployment of AI. Rather than measuring AI adoption through empirical or statistical variables, this study examines whether existing regulatory frameworks provide adequate legal safeguards for fundamental rights affected by AI-based systems [25]. The analysis is therefore directed toward identifying the extent to which principles such as human dignity, privacy, equality, non-discrimination, transparency, explainability, human oversight, accountability, and access to remedies are incorporated into AI governance frameworks [26]. This orientation is consistent with contemporary international AI governance, where human rights and human dignity have increasingly become central regulatory considerations. UNESCO, for example, identifies human rights and dignity as foundational elements of AI governance and emphasizes transparency, fairness, accountability, privacy, and human oversight across the AI lifecycle [27].

The comparative dimension is used to examine similarities, differences, and regulatory gaps among selected AI governance frameworks relevant to emerging economies. The frameworks are selected accord-

ing to four criteria: their substantive relevance to AI governance and digital human rights, their inclusion of provisions concerning risk and impact assessment, accountability, transparency, human oversight, data protection, or remedies, their relevance to emerging-economy regulatory conditions, and their institutional or legal significance in current international and national AI governance developments [28]. The comparison includes international normative instruments together with selected national and regional regulatory developments to identify how common human-rights principles are translated into operational or enforceable mechanisms [29]. These criteria are applied consistently across the selected materials to improve the transparency and reproducibility of the comparative legal analysis.

The study does not assume that a regulatory model developed in one jurisdiction can automatically be transferred to another jurisdiction. Instead, regulatory provisions are assessed in relation to institutional capacity, socioeconomic conditions, technological development, and the specific vulnerabilities experienced by populations in emerging economies [30]. The eight regulatory dimensions provide the detailed analytical criteria through which the comparative materials are assessed, while the four pillars synthesize the findings into a higher-level regulatory framework [31]. Privacy and data protection, together with equality and non-discrimination, are primarily integrated into the rights protection pillar. Risk assessment and risk management form the basis of risk governance. Accountability and institutional supervision are consolidated into institutional accountability, while transparency, explainability, human oversight, and access to remedies contribute to the operational requirements of the framework and support regulatory adaptability across different institutional contexts [32]. This analytical mapping enables the eight dimensions to function as detailed assessment criteria while the four pillars represent the principal regulatory outcomes derived from the comparative analysis. This approach is supported by recent international developments, including the Council of Europe's 2024 Framework Convention, which establishes a legally binding framework addressing AI across its lifecycle in relation to human rights, democracy, and the rule of law [33].

3.2. Legal Materials and Data Sources

The legal materials examined in this study consist of primary and secondary legal sources. Primary sources include international instruments, AI-related legislation, regulatory policies, official governmental documents, and institutional regulatory frameworks that directly address AI governance and digital human rights [34]. Particular attention is given to recent international frameworks because AI regulation has developed rapidly after 2022. The study considers international instruments such as the OECD AI Principles, United Nations Educational, Scientific and Cultural Organization (UNESCO's) recommendation on the Ethics of AI, and the Council of Europe Framework Convention on AI and Human Rights, Democracy and the Rule of Law [35]. These instruments provide different but complementary perspectives on AI governance. The OECD framework emphasizes transparency, explainability, safety, traceability, accountability, and continuous risk management, while UNESCO provides a broader human-rights-centered framework emphasizing dignity, privacy, fairness, inclusion, and human oversight [36].

Secondary legal materials comprise peer-reviewed academic publications, scholarly books, institutional reports, policy studies, and relevant legal commentaries published primarily between 2023 and 2026 [37]. The literature is selected based on its direct relevance to AI regulation, algorithmic accountability, digital human rights, data protection, algorithmic discrimination, AI governance, and emerging economies. Official institutional sources are prioritized when examining regulatory frameworks because they provide authoritative descriptions of current legal and policy instruments [38]. UNESCO's Ethical Impact Assessment is particularly relevant because it demonstrates how human-rights and ethical principles can be translated into an ex-ante assessment mechanism for AI systems.

3.3. Data Collection and Comparative Legal Analysis

The data collection process is conducted through documentary legal research. Relevant legal and policy documents are systematically identified, collected, screened, and categorized according to their relationship with AI governance and digital human rights [39]. The selection process focuses on documents that contain substantive provisions concerning AI development, deployment, monitoring, accountability, data processing, automated decision-making, algorithmic transparency, human oversight, or remedies [40]. Academic literature is selected using relevance and recency criteria, with priority given to publications from 2023 onward. The collected materials are subsequently organized according to major regulatory dimensions: privacy and data protection; equality and non-discrimination; transparency and explainability; human oversight; accountability; risk assessment; institutional supervision; and access to remedies.

The comparative analysis then examines how these dimensions are addressed across the selected regulatory frameworks. The comparison is not limited to the existence of legal provisions; it also evaluates their regulatory depth, enforceability, institutional responsibility, and practical applicability [41]. For example, a framework requiring transparency is considered more substantively developed when it specifies what information must be disclosed, to whom it must be disclosed, and how affected individuals can challenge an AI-generated decision. Similarly, accountability is assessed by examining whether responsibility is clearly assigned to developers, deployers, public authorities, or other relevant AI actors. This analytical strategy is consistent with the OECD approach, which links accountability with traceability of datasets, processes, and decisions and requires systematic risk management throughout the AI lifecycle [42].

3.4. Analytical Framework and Validity of the Research

The analytical framework is based on the premise that effective AI regulation should balance technological innovation, regulatory accountability, and fundamental rights [43]. Regulatory frameworks are evaluated across four interconnected dimensions: regulatory adequacy, assessing the clarity of legal obligations and safeguards; rights protection, examining privacy, dignity, equality, autonomy, freedom of expression, and procedural rights; institutional accountability, assessing the allocation of monitoring, auditing, enforcement, and remediation responsibilities; and contextual adaptability, considering the institutional, economic, technological, and social conditions of emerging economies [44].

The analysis is strengthened through source triangulation, comparing international standards with national legislation, academic literature, policy documents, and institutional reports. Consistent criteria are applied across jurisdictions to support systematic comparison, with particular attention to the distinction between formal regulatory adoption and substantive implementation. The existence of AI strategies or legal instruments does not necessarily ensure effective protection of digital human rights, as implementation gaps may remain in monitoring, impact assessment, evaluation, and institutional capacity [45].

The comparative findings are synthesized into a human-rights-centered regulatory framework for emerging economies, structured around four pillars: rights protection, risk governance, institutional accountability, and regulatory adaptability. These pillars provide practical safeguards for human-rights impact assessment, risk classification, transparency, documentation, auditing, and remedies, while enabling organizations and developers to implement risk assessment, human oversight, traceability, and continuous monitoring throughout the AI lifecycle.

4. RESULTS AND DISCUSSION

4.1. Regulatory Development of Artificial Intelligence and Human Rights Protection

The analysis indicates that AI regulation has progressively shifted from voluntary ethical principles toward structured, rights-oriented, and risk-based governance. Key principles include human dignity, autonomy, equality and non-discrimination, privacy and data protection, transparency, human oversight, accountability, and access to effective remedies. These developments show that AI regulation increasingly seeks not only to manage technological risks but also to ensure that AI systems remain consistent with fundamental rights throughout their lifecycle. A major development is the growing emphasis on risk and impact assessment before and during AI deployment. The 2024 Council of Europe Framework Convention requires AI-related activities to remain consistent with human rights, democracy, and the rule of law, while promoting assessment and mitigation of actual and potential impacts. This reflects a shift toward preventive AI governance.

Human oversight has also emerged as an essential safeguard, particularly for AI systems that significantly affect individuals. Technical accuracy alone cannot ensure legally or socially acceptable outcomes; human supervision enables automated decisions to be reviewed, challenged, and overridden when necessary. The analysis therefore identifies human oversight as a key link between technical governance and human-rights protection, especially in emerging economies with limited capacity to independently audit complex AI systems.

4.2. Comparative Assessment of AI Regulation and Digital Human Rights

The comparative analysis reveals that contemporary AI governance frameworks share a common normative foundation but differ substantially in regulatory depth, institutional mechanisms, and implementation requirements. International frameworks increasingly recognize that AI regulation must address both technological risks and their consequences for individuals. However, the existence of common principles does not necessarily result in uniform regulatory protection. Differences remain in how jurisdictions define high-risk

applications, allocate responsibility, establish oversight mechanisms, require impact assessments, and provide remedies to individuals affected by AI-based decisions.

Table 2. Comparative Regulatory Assessment of AI and Digital Human Rights

Regulatory Dimension	**International Regulatory Direction**	**Human Rights Implication**	**Key Finding for Emerging Economies**
Privacy and Data Protection	Increasing emphasis on responsible collection, processing, governance, and protection of personal data	Protects privacy, autonomy, and informational self-determination	Stronger data governance is required to prevent excessive or unlawful AI-driven data processing
Equality and Non-Discrimination	AI systems are increasingly expected to prevent discriminatory outcomes and reduce algorithmic bias	Protects equality and equal treatment	Emerging economies need mechanisms for detecting and mitigating algorithmic bias
Transparency and Explainability	Regulatory frameworks increasingly require information about AI systems and their decision-making processes	Supports autonomy, procedural fairness, and the ability to challenge decisions	Transparency requirements should be sufficiently practical for affected individuals, not limited to technical disclosure
Human Oversight	Human supervision is increasingly recognized as necessary for high-impact AI applications	Protects human autonomy, dignity, and due process	Institutional capacity to review and intervene in AI decisions must be strengthened
Accountability	Greater emphasis is placed on traceability, responsibility, auditing, and governance across the AI lifecycle	Provides mechanisms for assigning responsibility for harmful outcomes	Clear responsibilities among developers, deployers, regulators, and public institutions are essential
Risk and Impact Assessment	Risk-based and human-rights impact assessments are increasingly incorporated into AI governance	Enables preventive protection against foreseeable rights violations	Emerging economies require practical assessment mechanisms adapted to available institutional resources
Remedies and Redress	Affected persons increasingly receive procedural safeguards and opportunities to challenge AI-supported decisions	Strengthens access to justice and effective remedies	Regulatory frameworks should establish accessible complaint, review, and redress mechanisms

Table 2 demonstrates that the regulatory dimensions identified in the literature and methodology are increasingly reflected in contemporary AI governance. The strongest convergence occurs around privacy, non-discrimination, transparency, human oversight, accountability, and risk management. The Council of Europe Framework Convention provides particularly strong evidence of this convergence because it combines human

dignity, autonomy, equality, privacy, transparency, oversight, accountability, and safe innovation with procedural rights, complaints mechanisms, and risk and impact assessment.

However, the comparative findings highlight a gap between normative recognition and regulatory implementation. The inclusion of AI principles in legal instruments does not necessarily ensure effective protection in practice. In emerging economies, implementation depends on institutional capacity, technical expertise, financial resources, and regulatory coordination. Impact assessments, transparency, human oversight, auditability, and traceability can strengthen rights protection and accountability, but their effectiveness may be limited by insufficient expertise and institutional resources. Therefore, emerging economies need proportionate regulatory mechanisms that reflect available capacities while ensuring meaningful protection of digital human rights.

4.3. Regulatory Gaps in the Protection of Digital Human Rights

The analysis identifies four principal regulatory gaps affecting digital human rights protection in emerging economies. First, the implementation gap arises when broad AI governance principles lack effective enforcement, monitoring, and auditing mechanisms, creating a disconnect between regulatory objectives and practical outcomes. Second, the transparency and explainability gap reflects the limitations of technical disclosure. Meaningful transparency requires affected individuals to understand the role of AI, relevant decision factors, and available mechanisms to challenge harmful outcomes. Thus, transparency should function as a procedural right rather than merely a technical obligation.

Third, the institutional accountability gap results from the involvement of multiple actors across the AI lifecycle, including developers, providers, deployers, and public authorities. Clear allocation of responsibilities, supported by documentation, audits, supervision, and corrective measures, is therefore necessary to establish accountability. Fourth, the capacity gap reflects differences in infrastructure, expertise, financial resources, regulatory maturity, and institutional independence among emerging economies. Effective AI governance consequently requires both strong legal safeguards and sufficient institutional and technical capacity for implementation.

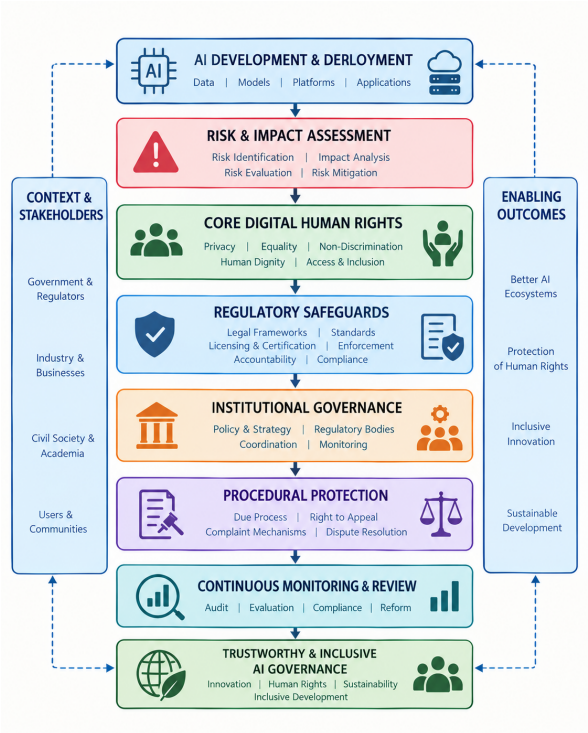


Figure 1. Human-Rights-Centered AI Regulatory Framework for Emerging Economies

Figure 1 illustrates the human-rights-centered regulatory framework developed from the comparative findings. It brings together risk assessment, digital human rights, regulatory safeguards, institutional governance, procedural protection, and continuous monitoring within a single regulatory structure. The figure

further operationalizes the four-pillar framework by illustrating how rights protection, risk governance, institutional accountability, and regulatory adaptability are connected throughout the AI lifecycle. Rather than functioning as separate regulatory elements, these four pillars are presented as interdependent mechanisms through which human-rights principles can be translated into concrete safeguards, institutional duties, and accountability measures.

Within this structure, institutional governance is positioned between regulatory safeguards and procedural protection. This arrangement reflects the finding that legal principles require capable institutions to support their implementation, monitoring, and enforcement. Procedural safeguards, including notification, the right to challenge AI-supported decisions, complaint mechanisms, and access to effective remedies, provide individuals with practical avenues to protect and exercise their rights when affected by AI systems. Continuous monitoring and periodic review then support the adaptability of the regulatory framework by allowing governance arrangements to respond to changes in technology, emerging risks, and evolving social contexts. This lifecycle-oriented structure is consistent with the 2024 Council of Europe approach, which emphasizes rights-consistent AI governance across the AI lifecycle and links fundamental principles with risk assessment, procedural safeguards, and mechanisms for implementation and monitoring.

4.4. Human-Rights-Based Regulatory Framework for Emerging Economies

The final finding of this study is that an effective regulatory model for emerging economies should be constructed around four interconnected pillars: rights protection, risk governance, institutional accountability, and regulatory adaptability. The first pillar requires the explicit integration of digital human rights into AI regulation. Privacy, equality, non-discrimination, dignity, autonomy, freedom of expression, and procedural fairness should not be treated as secondary ethical considerations but as substantive regulatory requirements. The second pillar is risk-based governance. AI applications should be assessed according to the potential severity and likelihood of their impact on individuals and society. Higher-risk applications should consequently be subject to stronger requirements for impact assessment, documentation, human oversight, monitoring, and accountability. This approach is consistent with the Council of Europe's emphasis on assessing actual and potential impacts on human rights, democracy, and the rule of law.

The third pillar is institutional accountability. Emerging economies need clearly defined responsibilities among regulators, public authorities, developers, deployers, and other AI actors. Accountability should be supported by independent supervision, auditability, traceability, documentation, and accessible complaint mechanisms. The analysis demonstrates that accountability is particularly important where individuals have limited technical ability to independently evaluate AI systems. The fourth pillar is regulatory adaptability. AI regulation should be sufficiently flexible to respond to technological change while maintaining stable human-rights protections. A technology-neutral approach can reduce the risk that regulation becomes obsolete as AI systems evolve. The Council of Europe Framework Convention adopts this approach by establishing rights-based obligations without regulating a specific technology, thereby seeking to remain applicable as technological developments continue.

Overall, the findings demonstrate that the central regulatory challenge for emerging economies is not simply whether AI should be regulated, but how AI can be governed in a manner that simultaneously promotes innovation and guarantees effective digital human rights protection. The results support a shift from fragmented, principle-based governance toward an integrated regulatory architecture combining risk assessment, substantive rights protection, institutional accountability, procedural safeguards, and continuous monitoring. Such an approach provides a more appropriate foundation for emerging economies because it recognizes that effective AI governance depends not only on legal norms but also on institutional capacity and the ability of individuals to exercise meaningful rights when AI systems affect their lives.

5. MANAGERIAL IMPLICATIONS

The findings provide important managerial implications for policymakers, regulators, public institutions, and organizations deploying AI in emerging economies. Managers and institutional decision-makers should move beyond treating AI governance as a purely technical or compliance-oriented responsibility and instead integrate digital human rights into organizational risk management and strategic decision-making. In practice, organizations should establish clear AI governance mechanisms covering privacy and data protection, algorithmic transparency, explainability, non-discrimination, human oversight, accountability, and continuous

risk assessment throughout the AI lifecycle. Before deployment, managers should conduct documented risk and human-rights impact assessments and define responsibilities for high-impact AI systems. During deployment, organizations should maintain documentation and audit trails, establish qualified human oversight with authority to review or intervene in AI-supported decisions, and conduct periodic audits of system performance, risks, and potential discriminatory effects. Organizations should also provide accessible complaint and review mechanisms through which affected individuals can request explanations, challenge AI-supported decisions, and obtain appropriate remedies. These measures translate the proposed four-pillar framework into organizational governance practices and strengthen accountability beyond formal regulatory compliance. Particular attention should be given to high-impact AI applications, where organizations should conduct human-rights and impact assessments before deployment, maintain appropriate documentation and audit trails, and provide accessible mechanisms through which affected individuals can request explanations, challenge AI-supported decisions, and obtain appropriate remedies. For emerging economies, these measures should be accompanied by investments in regulatory and managerial capabilities, including employee training, independent oversight, cross-functional governance teams, and collaboration among government agencies, technology providers, civil society, and other stakeholders. Such an approach enables organizations to manage AI-related risks more systematically while maintaining public trust, supporting responsible innovation, and ensuring that digital transformation contributes to inclusive economic and social development rather than reinforcing existing inequalities.

6. CONCLUSION

This study concludes that AI regulation in emerging economies requires a shift from technology-centered governance toward a human-rights-centered regulatory approach. The findings show that contemporary AI governance increasingly addresses privacy and data protection, equality and non-discrimination, transparency, explainability, human oversight, accountability, risk assessment, and access to remedies. However, significant implementation gaps remain due to differences in institutional capacity, regulatory maturity, technological infrastructure, technical expertise, and enforcement mechanisms. The theoretical contribution of this study is the development of a four-pillar regulatory framework encompassing rights protection, risk governance, institutional accountability and regulatory adaptability. This framework integrates substantive human-rights protection with preventive risk governance, defined institutional responsibilities and context-sensitive regulatory adaptation. In practical terms, it provides guidance for regulators, public institutions and organizations to implement risk and human-rights impact assessments, transparency and documentation requirements, human oversight, auditing, accountability mechanisms and accessible remedies throughout the AI lifecycle. The analysis demonstrates that the existence of regulatory principles alone does not guarantee effective protection of digital human rights, particularly in emerging economies facing institutional and regulatory constraints. The proposed framework therefore emphasizes the need to manage technological risks, protect fundamental rights, strengthen institutional responsibility and maintain flexibility to support responsible innovation and inclusive digital development.

In response to the research question concerning how AI regulation can protect digital human rights in emerging economies, the study finds that effective protection depends on the integration of human-rights principles into enforceable regulatory and institutional mechanisms throughout the AI lifecycle. Regulatory frameworks should require appropriate risk and human-rights impact assessments, transparency and explainability, meaningful human oversight, clear allocation of responsibility, continuous monitoring, and accessible mechanisms for challenging AI-supported decisions and obtaining remedies. The study therefore confirms that AI regulation should be evaluated not merely according to the existence of legislation or policy instruments, but according to their capacity to produce meaningful and enforceable rights protection. Nevertheless, this study has limitations. As a normative and comparative legal study, it relies primarily on legal documents, regulatory instruments, academic literature, and institutional reports and therefore does not empirically measure the actual experiences of individuals, organizations, regulators, or AI developers in emerging economies. In addition, differences in legal systems, institutional capacity, and national contexts limit the extent to which the proposed framework can be applied uniformly across all emerging economies.

Future research should therefore extend this study through empirical, comparative, and interdisciplinary approaches that examine how AI regulations are implemented in specific emerging-economy contexts. Quantitative and qualitative studies involving policymakers, regulators, technology developers, businesses, and affected communities could provide evidence regarding the effectiveness of transparency requirements, algo-

rithmic impact assessments, human oversight, accountability mechanisms, and available remedies in practice. Future studies should also conduct country-level comparative research to identify how differences in institutional capacity, digital infrastructure, data protection regimes, and regulatory enforcement influence the effectiveness of AI governance. Furthermore, subsequent research could develop measurable indicators for evaluating the maturity of human-rights-based AI regulation and empirically test the four-pillar framework proposed in this study. Particular attention should also be given to emerging technologies such as generative AI and increasingly autonomous AI systems, whose rapid development may create new challenges for privacy, discrimination, accountability, and human autonomy. Such research would strengthen the empirical foundation of AI governance and contribute to the development of adaptive, inclusive, and rights-preserving regulatory frameworks capable of balancing technological innovation with the protection of digital human rights in emerging economies.

7. DECLARATIONS

7.1. About Authors

Marviola Hardini (MH) https://orcid.org/0000-0003-3336-2131

Richard Andre Sunarjo (RS) https://orcid.org/0009-0007-7349-2375

Nyree Ani (NA) https://orcid.org/0009-0009-0623-1911

Apriani Sijabat (AS) https://orcid.org/0000-0002-0044-052X

7.2. Author Contributions

Conceptualization: MH; Methodology: AS; Software: NA; Validation: RS, MH and NA; Formal Analysis: AS and RS; Investigation: MH; Resources: NA; Data Curation: RS and NA; Writing – Original Draft Preparation: MH and NA; Writing Review and Editing: AS and RS; Visualization: MH; All authors, MH, RS, NA and AS, have read and agreed to the published version of the manuscript.

7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.5. Institutional Review Board Statement

Not applicable.

7.6. Informed Consent Statement

Not applicable.

7.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

[1] M. Hakimi, S. Zarinkhail, and F. A. Sahnosh, "Artificial intelligence and legal reform in developing countries: Advancing ethical, rights-based, and accountable digital governance," *Jurnal Ilmiah Telsinas Elektro, Sipil dan Teknik Informasi*, vol. 8, no. 2, pp. 127–144, 2025.

[2] A. K. Sharma and R. Sharma, "Governance in the age of artificial intelligence: A comparative analysis of policy framework in brics nations," *Ai Magazine*, vol. 46, no. 2, p. e70010, 2025.

[3] N. Lutfiani, S. Wijono, U. Rahardja, A. Iriani, and E. A. Nabila, "Artificial intelligence based on recommendation system for startup matchmaking platform," in *2022 IEEE Creative Communication and Innovative Technology (ICCIT)*. IEEE, 2022, pp. 1–5.

[4] P. C. Aloamaka, M. O. Omozue *et al.*, "Ai and human rights: navigating ethical and legal challenges in developing nations," *Khazanah Hukum*, vol. 6, no. 2, pp. 189–201, 2024.

[5] A. Barzelay, J. Ng, and M. Romanoff, "Governing artificial intelligence responsibility in low to middle income countries: Enabling pathways to sustainable development," *Cal. W. Int'l LJ*, vol. 54, p. 415, 2023.
[6] N. Nuryani, A. B. Mutiara, I. M. Wiryana, D. Purnamasari, and S. N. W. Putra, "Artificial intelligence model for detecting tax evasion involving complex network schemes," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 3, pp. 339–356, 2024.
[7] A. Monasterio Astobiza, T. Ausín, B. Liedo, M. Toboso, M. Aparicio, and D. López, "Ethical governance of ai in the global south: A human rights approach to responsible use of ai," in *Proceedings*, vol. 81, no. 1. MDPI, 2022, p. 136.
[8] C. T. Okolo and M. Raji, "The global majority in international ai governance," in *Handbook on the Global Governance of Artificial Intelligence*. Edward Elgar Publishing, 2026, pp. 133–154.
[9] R. Salam, Q. Aini, B. A. A. Laksminingrum, B. N. Henry, U. Rahardja, and A. A. Putri, "Consumer adoption of artificial intelligence in air quality monitoring: A comprehensive utaut2 analysis," in *2023 Eighth International Conference on Informatics and Computing (ICIC)*. IEEE, 2023, pp. 1–6.
[10] Y. Walter, "Managing the race to the moon: Global policy and governance in artificial intelligence regulation—a contemporary overview and an analysis of socioeconomic consequences," *Discover Artificial Intelligence*, vol. 4, no. 1, p. 14, 2024.
[11] N. Singh and L. Krishnaiah, "The governance of ai from 16 diverse ethical perspectives," *Handbook of Global Philosophies on AI Ethics: Toward Sustainable Futures*, vol. 216, 2025.
[12] J. Juanda, R. J. Riansyah, A. Arsadi, and L. Bethany, "Towards entrepreneurial campus sustainability: Integrating artificial intelligence for resource allocation in business management," *Aptisi transactions on technopreneurship (ATT)*, vol. 6, no. 3, pp. 314–323, 2024.
[13] A. B. d. C. da Conceição and S. Suhermin, "Bridging ethics and innovation in artificial intelligence: A human-centered approach to responsible technology design," in *International Conference of Business and Social Sciences*, 2025, pp. 206–214.
[14] M. Chinen, "International governance of ai," in *Handbook of Human-Centered Artificial Intelligence*. Springer, 2026, pp. 1821–1857.
[15] S. Kosasi, C. Lukita, M. H. R. Chakim, A. Faturahman, and D. A. R. Kusumawardhani, "The influence of digital artificial intelligence technology on quality of life with a global perspective," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 240–250, 2023.
[16] M. A. Santoro and B. D. Stone, "Artificial intelligence, human rights, and the future of work: Global governance and international organizations in the age of ai," *Journal of Human Rights*, pp. 1–17, 2026.
[17] M. Campbell, "A values-driven data protection framework for ai adoption in emerging economies," *ScienceOpen Preprints*, 2026.
[18] H. Herman, N. P. L. Santoso, A. Avandi, N. Septiani, and O. Sy, "Legal governance of artificial intelligence in sustainable digital business ecosystems," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 209–221, 2026.
[19] H. Roberts, E. Hine, M. Taddeo, and L. Floridi, "Global ai governance: barriers and pathways forward," *International Affairs*, vol. 100, no. 3, pp. 1275–1286, 2024.
[20] M. S. Khan, H. Umer, and F. Faruqe, "Artificial intelligence for low income countries," *Humanities and Social Sciences Communications*, vol. 11, no. 1, p. 1422, 2024.
[21] I. Haryanto, Y. Yunadin, W. Setiawan, F. Agrimiandra, and D. Alam, "Legal governance of technology driven cybercrime in digital society," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 141–154, 2026.
[22] F. S. Sedeeq and P. Arman, "Human-centric ai governance: An adaptive public international law framework for ethical and inclusive ai regulation in public health," *Journal of Law, Medicine & Ethics*, vol. 53, no. 4, pp. 563–574, 2025.
[23] A. Sigfrids, J. Leikas, H. Salo-Pöntinen, and E. Koskimies, "Human-centricity in ai governance: A systemic approach," *Frontiers in artificial intelligence*, vol. 6, p. 976887, 2023.
[24] P. Paroli, A. Rizky, Q. Aini, D. Cahyono, J. Parker, and U. Rahardja, "Artificial intelligence driven predictive risk management in green technology investment," *APTISI Transactions on Management*, vol. 10, no. 2, pp. 203–214, 2026. [Online]. Available: https://doi.org/10.33050/cz38xg11
[25] D. Mhlanga, "Human-centered artificial intelligence: The superlative approach to achieve sustainable development goals in the fourth industrial revolution," *Sustainability*, vol. 14, no. 13, p. 7804, 2022.
[26] A. O. Aderibigbe, P. E. Ohenhen, N. K. Nwaobia, J. O. Gidiagba, and E. C. Ani, "Artificial intelligence

in developing countries: Bridging the gap between potential and implementation," *Computer Science & IT Research Journal*, vol. 4, no. 3, pp. 185–199, 2023.

[27] E. S. Pramudito, R. Widayanti, S. Purnama, and K. A. Al-Farouqi, "Reinventing human resource practices through digital marketing platforms and remote work technologies," *APTISI Transactions on Management*, vol. 9, no. 3, pp. 267–277, 2025. [Online]. Available: https://doi.org/10.33050/atm.v9i3.2540

[28] United Nations, "Global dialogue on ai governance: Frequently asked questions," https://www.un.org/global-dialogue-ai-governance/en/faq, 2026, accessed: September 28, 2026.

[29] E. Zaidan and I. A. Ibrahim, "Ai governance in a complex and rapidly changing regulatory landscape: A global perspective," *Humanities and Social Sciences Communications*, vol. 11, no. 1, 2024.

[30] M. Mustam, A. Rizky, and J. Edwards, "Technology innovation adoption for business performance in the digital economy," *APTISI Transactions on Management*, vol. 10, no. 3, pp. 332–345, 2026. [Online]. Available: https://doi.org/10.33050/9ncj5227

[31] O. Ozmen Garibay, B. Winslow, S. Andolina, M. Antona, A. Bodenschatz, C. Coursaris, G. Falco, S. M. Fiore, I. Garibay, K. Grieman *et al.*, "Six human-centered artificial intelligence grand challenges," *International Journal of Human–Computer Interaction*, vol. 39, no. 3, pp. 391–437, 2023.

[32] B. G. Mujtaba *et al.*, "Human-ai intersection: Understanding the ethical challenges, opportunities, and governance protocols for a changing data-driven digital world," *Business Ethics and Leadership*, vol. 9, no. 1, pp. 109–126, 2025.

[33] U.S. Department of State, "Risk management profile for artificial intelligence and human rights," Bureau of Cyberspace and Digital Policy, U.S. Department of State, Risk Management Profile, Jul. 2024. [Online]. Available: https://2021-2025.state.gov/risk-management-profile-for-ai-and-human-rights/

[34] W. Holmes, J. Persson, I.-A. Chounta, B. Wasson, and V. Dimitrova, *Artificial intelligence and education: A critical view through the lens of human rights, democracy and the rule of law*. Council of Europe, 2022.

[35] A. Rachovitsa and N. Johann, "The human rights implications of the use of ai in the digital welfare state: Lessons learned from the dutch syri case," *Human Rights Law Review*, vol. 22, no. 2, p. ngac010, 2022.

[36] C. Lukita, A. K. Chandra, R. Fahrudin, N. M. Agatha, and D. P. Suci, "Maturity level measurement model of msmes for sustainable economic growth," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 2, pp. 434–442, 2026.

[37] J. N. Sheth, V. Jain, G. Roy, and A. Chakraborty, "Ai-driven banking services: the next frontier for a personalised experience in the emerging market," *International Journal of Bank Marketing*, vol. 40, no. 6, pp. 1248–1271, 2022.

[38] K. Abrokwah-Larbi and Y. Awuku-Larbi, "The impact of artificial intelligence in marketing on the performance of business organizations: evidence from smes in an emerging economy," *Journal of Entrepreneurship in Emerging Economies*, vol. 16, no. 4, pp. 1090–1117, 2024.

[39] J. B. Hendrawidjaja, B. W. Soetjipto, R. D. Kusumastuti, and O. Jayanagara, "Ecosystem exchange, strategic capabilities, and firm performance with agility and innovation mediators," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 226–238, 2026.

[40] K. Patel, "Ethical reflections on data-centric ai: balancing benefits and risks," *International Journal of Artificial Intelligence Research and Development*, vol. 2, no. 1, pp. 1–17, 2024.

[41] A. Poo-Udom, "The primacy of ethical governance: Unraveling the ai-hrm adoption paradox in an emerging economy," *Social Sciences & Humanities Open*, vol. 14, p. 103554, 2026.

[42] F. Cloete, "Governing artificial intelligence (ai) and other technologies in the digital era," *Administratio Publica*, vol. 32, no. 1, pp. 1–30, 2024.

[43] C. Yılmaz, "The geopolitics of artificial intelligence: Power, regulation, and global governance," *UFÜ Sosyal ve Beşeri Bilimler Dergisi*, vol. 2, no. 3, pp. 39–70, 2026.

[44] V. Gaur and N. Jamal, "Human rights and artificial intelligence: Addressing emerging threats to humanity in indian context," *International Journal of Social Science Research (IJSSR)*, vol. 2, no. 4, pp. 640–650, 2025.

[45] H. Chen, "The ethical challenges of educational artificial intelligence and coping measures: A discussion in the context of the 2024 world digital education conference." *Science Insights Education Frontiers*, vol. 20, no. 2, p. 3263, 2024.