International Journal of Law Analytics (IJLA)
Vol. 4, No. 4 2026: 633-652

Legal Challenges and the CAPRI-AI Governance Model in Developing Countries: A Comparative Study of Eight Jurisdictions

Kurniawan Tri Wibowo[1]*, Firman Muhammad Arif[2], Habibi Abdul Jalil[3]
[1]Universitas AMIKOM Purwokerto
[2]Universitas Islam Negeri (UIN) Palopo
[3]Universitas Sebelas Maret
Corresponding Author: Kurniawan Tri Wibowo
kurniawan@amikompurwokerto.ac.id

A R T I C L E I N F O

Keywords: Artificial Intelligence, AI Regulation, Developing Countries, AI Governance, Normative Legal Research

Received : 15, July
Revised : 16, September
Accepted: 17, November

©2026 Wibowo, Arif, Jalil: This is an open-access article distributed under the termsof the Creative Commons Atribusi 4.0 Internasional.

A B S T R A C T

This study examines AI governance in eight jurisdictions: Indonesia, India, Brazil, South Africa, Kenya, Malaysia, the Philippines, and the Netherlands, to identify regulatory patterns, explain governance-design differences, and formulate a capacity-sensitive model for developing jurisdictions. Using qualitative normative legal research, it applies statutory, conceptual, and functional-comparative approaches. A purposive corpus of 57 legal, policy, institutional, and scholarly documents was analysed through structured review matrix and qualitative content analysis across five dimensions: legal architecture, data governance, lifecycle accountability, rights and remedies, and institutional capacity. Divergence reflects policy objectives, data-protection and administrative-law maturity, institutional and technical capacity, foreign AI-infrastructure dependence, and regional/supranational policy influence. CAPRI-AI comprises capacity-calibrated implementation, accountable lifecycle allocation, proportionate risk classification, rights- and data-based safeguards, and iterative institutional learning.

DOI: https://doi.org/10.59890/ijla.v4i4.326
E-ISSN: 3032-4041
https://slamultitechpublisher.my.id/index.php/ijla

INTRODUCTION

Artificial intelligence (AI) has become part of the infrastructure of public administration, finance, health, education, employment, trade, policing, and information production. AI systems can classify people, generate content, recommend action, and support or automate decisions with legal and social consequences. These capabilities improve efficiency and expand access to services, but they also create risks of privacy invasion, discriminatory profiling, unsafe outputs, manipulation, intellectual-property disputes, and uncertainty about responsibility. The regulatory challenge is particularly acute in developing countries, where adoption can outpace legislation, regulatory expertise, audit infrastructure, and accessible remedies (Chattopadhyay & Foster, 2025).

The central problem is not merely the absence of an AI Act. In many jurisdictions, legally relevant obligations already exist in data-protection, electronic-transactions, cybersecurity, consumer, employment, administrative, competition, and intellectual-property law. The difficulty is that these norms are fragmented, apply to different actors, and rarely provide a coherent lifecycle structure for training data, risk classification, model testing, deployment, monitoring, explanation, human review, and redress. Arvante et al. (2025) argues that digital law must be adaptive and function as an instrument of social engineering rather than remain a collection of static norms. Similarly, Fischer (2023) place privacy and data governance at the centre of legal responses to emerging digital technologies. These insights support the proposition that AI governance must link normative protection to operational institutions.

Indonesia illustrates this tension. Law Number 27 of 2022 concerning Personal Data Protection, Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transaction Law, Government Regulation Number 71 of 2019, and the Ministerial Circular on AI Ethics provide an initial basis for legality, security, accountability, and data-subject rights. Nevertheless, they do not yet establish a comprehensive classification of AI risks, mandatory algorithmic impact assessment, audit standards, a public-sector AI register, or a complete allocation of duties among developers, providers, deployers, professional users, and procuring institutions. The Pancasila-based approach proposed by Kang & Havercroft (2025) supplies an important normative foundation, while Bennett (2025) demonstrates that ambiguity becomes especially harmful where AI affects employment and individual rights.

As of August 2026, Indonesia remains without a comprehensive AI statute, but its regulatory trajectory has moved beyond the earlier fragmented policy stage. The government has been developing two Presidential Regulations concerning AI ethics and the National AI Roadmap for 2026–2029. Cross-ministerial deliberation on both draft regulations was completed in May 2026, indicating an ongoing transition toward a more consolidated national governance architecture. These developments do not yet amount to a comprehensive statutory AI regime; rather, they demonstrate an incremental regulatory strategy that seeks to coordinate existing legal instruments before moving toward broader legislation. This trajectory is particularly relevant to a capacity-sensitive approach because it illustrates how governance obligations

may be introduced progressively while institutional arrangements are being developed.

A comparison limited to Indonesia, India, Brazil, South Africa, and Kenya reveals broad Global South patterns, but it risks producing a descriptive catalogue. This study therefore retains those five core jurisdictions and adds Malaysia and the Philippines as peer ASEAN comparators with more directly transferable regulatory and institutional conditions. It also uses the Netherlands as a functional benchmark because its civil-law setting, public algorithm register, supervisory coordination, and implementation of the European Union Artificial Intelligence Act provide a mature reference point. The Netherlands is not treated as economically equivalent to the developing countries; it is used to identify which institutional functions can be adapted and which resource-intensive components should not be transplanted wholesale.

Previous studies have examined AI-specific regulation, legal personality, data protection, employment, public policy, copyright, and criminal responsibility. Gardi & Eddine (2023) emphasises the urgency of specific rules for personal-data protection, Wen & Tong (2023) examine AI as a possible legal subject; Alnaim (2025) analyses adaptive policy; Jun et al. (2023) propose comparative risk-based recommendations; and Plantinga et al. (2023) advocate rights-based governance tailored to developing-country capacity. However, these strands are often separated, and comparative studies frequently describe national instruments without explaining the causes of divergence or converting the comparison into an original governance model.

This study addresses three research questions. First, what are the principal strengths and weaknesses of AI governance in the eight selected jurisdictions? Second, why do their regulatory pathways differ, and what causal factors explain those differences? Third, what conceptual governance model can be derived for developing countries, particularly Indonesia? The study makes four scientific contributions: it develops a comparative typology of AI regulatory pathways; identifies causal variables behind regulatory divergence; constructs a lifecycle accountability framework; and formulates the CAPRI-AI model as a capacity-calibrated, risk-based, rights-oriented, and iterative architecture. The novelty therefore lies not simply in adding countries, but in converting comparative findings into a testable conceptual and normative model.

THEORETICAL REVIEW

Responsive Law, Digital Law, and Institutional Capacity

Responsive legal theory views law as a purposive institution that must remain open to social needs, participation, and changing conditions. Applied to AI, responsiveness requires anticipatory safeguards before harm occurs and revision mechanisms after technologies, markets, or social effects change. Cao et al. (2025) extends this logic to digital law by emphasising adaptability, transparency, accountability, and sustainability. This approach rejects both technological determinism and purely reactive legislation: the legal system must shape innovation while preserving human dignity and public trust.

Institutional capacity qualifies the promise of responsive law. A rule requiring an algorithmic audit is ineffective where regulators lack access to documentation, qualified auditors, testing facilities, or sanctioning power. Conversely, a detailed legal framework can generate symbolic compliance and disproportionate burdens where obligations are not matched to state and industry capacity. The analysis therefore treats legal completeness and implementation capacity as separate but interdependent variables.

Risk-Based, Rights-Based, and Lifecycle Governance

Risk-based regulation differentiates obligations according to the severity, probability, scale, reversibility, and social context of harm. Low-risk systems may require basic notice and security, while systems used in health, education, employment, credit, biometrics, essential public services, and law enforcement may require impact assessment, data testing, technical documentation, human oversight, independent audit, and contestability. Heo et al. (2024) show that Indonesia has not yet adopted comprehensive risk classification, while Bourgeois et al. (2024) stress that risk tiers in developing countries must consider resource limitations and unequal access to remedies.

Rights-based governance focuses on the legal position of affected persons: notice, lawful data processing, non-discrimination, meaningful explanation, human review, objection, and effective remedy. Data governance is not reducible to consent because model training can involve repurposing, inferred data, publicly accessible personal information, group harms, and cross-border datasets. Emon (2026) underline the need to connect privacy protection with transparency, security, and institutional responsibility. Lifecycle governance allocates responsibility across design, data collection, model training, integration, deployment, professional use, monitoring, and retirement. The responsibility-gap literature explains why AI harm can be difficult to attribute to a single actor (Königs, 2022). Lim (2025) similarly frame responsible AI governance as an organisational system involving structures, procedures, controls, and stakeholder participation. These perspectives favour responsibility based on control, knowledge, benefit, and ability to prevent harm rather than granting AI independent legal personality.

Comparative Regulatory Pathways and Research Gap

Developing countries have adopted three broad pathways. The first is fragmented statutory governance, in which data-protection and sectoral laws indirectly regulate AI. The second is strategy- or guideline-led governance, which promotes innovation and ethical principles but lacks binding remedies. The third is emerging risk-based legislation, which seeks to classify systems and impose differentiated duties. Brazil approaches the third pathway; India, Kenya, South Africa, Malaysia, and the Philippines combine the first two in different forms; and Indonesia remains largely fragmented and policy-driven. The Netherlands, operating within the EU framework, demonstrates a more mature combination of binding risk rules, supervisory coordination, public transparency instruments, and institutional learning.

Novelli et al. (2024) connect unclear AI status with accountability problems, while Maria and Riswadi (2024) note that national strategies do not have the binding force of legislation. De Vries (2023) show similar uncertainty in criminal responsibility. Although Lovell (2023) explore AI legal personality, this study treats personhood as a secondary debate and prioritises enforceable human and corporate responsibility. The remaining research gap is explanatory and constructive: existing work rarely explains why regulatory differences emerge or derives a capacity-sensitive governance model from those differences.

Conceptual Framework

The analytical framework consists of five substantive dimensions. The first is legal architecture: definitions, legal force, risk classification, prohibited practices, standards, and regulatory coordination. The second is data governance: lawful basis, purpose limitation, data quality, representativeness, security, cross-border transfer, and data-subject rights. The third is lifecycle accountability: allocation of duties among developers, data providers, application providers, deployers, operators, professional users, and procuring institutions. The fourth is rights and remedies: notice, explanation, human review, objection, complaint, compensation, and correction. The fifth is institutional capacity: expertise, audit infrastructure, authority, budget, access to evidence, coordination, and international cooperation.

To move beyond description, the study also codes five explanatory variables: the dominant regulatory objective, ranging from innovation promotion to rights protection; maturity of data-protection and administrative law; state and market capacity; dependence on foreign models and cloud infrastructure; and regional or supranational normative pressure. These variables are used to explain why jurisdictions with similar risks produce different legal responses.

METHODOLOGY

Research Design and Jurisdiction Selection

This research uses a qualitative normative legal method with statutory, conceptual, and functional-comparative approaches. The statutory approach examines legislation, regulations, official strategies, guidelines, and regulatory instruments. The conceptual approach examines responsive law, risk-based regulation, rights-based governance, responsibility gaps, and institutional capacity. The comparative approach asks how different legal systems perform equivalent governance functions rather than merely comparing formal wording (Giest & Klievink, 2024).

Indonesia is the anchor jurisdiction. India, Brazil, South Africa, and Kenya represent large or influential developing economies across Asia, Latin America, and Africa with varying digital capacity and AI-policy maturity. Malaysia and the Philippines are selected as peer ASEAN comparators because their administrative capacity, regional commitments, and data-governance challenges are more directly comparable with Indonesia. The Netherlands is selected as a benchmark rather than a peer: its value lies in demonstrating how binding risk regulation, algorithmic transparency, and coordinated supervision operate in a resource-rich civil-law environment. This combination applies both a most-

similar logic among ASEAN states and a most-different logic between developing jurisdictions and the Dutch/EU benchmark.

Population, Sample, and Document Selection

The population includes legislation, official policies, international and regional instruments, books, scientific articles, and institutional reports concerning AI governance, personal data, electronic systems, consumer protection, accountability, transparency, and institutional readiness. Purposive sampling was based on relevance, authority, validity, availability of full text, and contribution to the analytical dimensions. The final corpus contains 57 documents: 45 core documents from the original five-country analysis and 12 comparator materials added for Malaysia, the Philippines, the Netherlands, ASEAN, the European Union, and the authors' digital-law scholarship.

Table 1. Composition of the Analysed Documents

Document category	Number
National legal and policy documents in the five core jurisdictions	25
Comparator legal and policy documents: Malaysia, Philippines, and Netherlands	8
International and regional instruments	10
Scientific articles, books, and policy reports	14
Total	57

Primary legal materials were included whenever valid or relevant. Secondary materials were generally limited to 2021–2026 to maintain analytical currency, while foundational legal and institutional materials were included where necessary. Duplicate publications, non-authoritative opinion pieces, unidentified sources, and documents dealing only with technical performance were excluded.

Data Collection and Analysis

Documents were located through official government and institutional websites and academic databases, including Scopus, Web of Science, Google Scholar, HeinOnline, SpringerLink, and ScienceDirect. Search terms included "AI regulation," "AI governance," "algorithmic accountability," "risk-based regulation," "automated decision-making," "data protection," and the names of the selected jurisdictions. The review matrix recorded legal status, scope, AI definition, risk tier, data duties, transparency, accountability, human oversight, supervisory authority, audit, sanctions, and remedies. Content analysis was conducted in two cycles. The first cycle used deductive coding based on the five substantive dimensions. The second used axial coding to identify explanatory patterns linking legal outcomes to regulatory purpose, legal maturity, capacity, technological dependence, and external policy pressure. Comparative legal analysis then identified functional equivalents, institutional gaps, advantages, disadvantages, and transferable lessons. NVivo 14 supported coding, Microsoft Excel 2021 supported the document matrix, and Mendeley Reference Manager

supported citation management. Source triangulation compared legal texts, official policy documents, institutional reports, and scholarly literature (Raimi, 2026).

RESEARCH RESULTS

Comparative Regulatory Architecture: Strengths and Weaknesses

The comparison reveals four regulatory postures rather than a simple division between countries with and without AI legislation: fragmented statutory governance, innovation-led soft law, emerging risk-based legislation, and integrated risk-and-rights governance. Each posture has advantages and weaknesses. Fragmented systems can use existing law quickly but create gaps and coordination problems. Soft-law systems are flexible and innovation-friendly but often lack enforceable remedies. Risk-based bills offer coherence but face legislative delay and compliance demands. Mature integrated systems improve accountability but require high administrative and technical capacity.

Table 2. Comparative Strengths, Weaknesses, and Explanatory Factors

Jurisdiction	Regulatory posture	Principal strengths	Principal weaknesses and explanation
Indonesia	Fragmented statutory and ethics-guideline model	PDP Law, electronic-systems duties, constitutional and Pancasila-oriented values; flexible sectoral entry points.	No unified risk tiers, mandatory impact assessment, audit standard, or clear lifecycle responsibility. Fragmentation reflects dispersed authority and rapid adoption ahead of specialist capacity.
India	Innovation-led, sectoral, and increasingly guideline-based	Large digital public infrastructure, strong innovation ecosystem, evolving governance guidelines, and capacity-building initiatives.	Limited horizontal enforceability and uneven transparency across sectors. Policy prioritises scale, inclusion, and innovation while avoiding premature comprehensive legislation.
Brazil	Emerging rights- and risk-based legislative model	LGPD foundation, legislative attention to rights, high-risk uses, duties, and civil responsibility; stronger public debate.	Bill implementation remains institutionally demanding; federal and sectoral coordination and compliance costs are significant. Rights-oriented constitutional and data-protection traditions push toward comprehensive rules.
South Africa	Data-protection and transformative-policy model	POPIA and constitutional equality provide a rights foundation; policy discourse	AI-specific obligations, audit capacity, and coordinated enforcement remain limited. Socio-economic inequality and uneven public-sector capacity complicate implementation.

		recognises inclusion and transformation.	
Kenya	National strategy and innovation-hub model	2025–2030 strategy links AI to national development, local innovation, skills, infrastructure, and responsible governance.	Strategy requires conversion into enforceable duties, audit standards, and accessible remedies. Growth-oriented policy and resource constraints favour staged implementation.
Malaysia	Pragmatic standards- and guideline-led ASEAN peer	National Guidelines on AI Governance and Ethics provide lifecycle roles, risk management, ethical principles, and alignment with international standards.	Predominantly non-binding and organisation-centred; individual rights, sanctions, independent audit, and remedies are less developed. Strong administrative coordination supports pragmatic soft law.
Philippines	Privacy-regulator-led ASEAN peer	NPC Advisory No. 2024-04 operationalises transparency, accountability, privacy impact assessment, data minimisation, lawful basis, and data-subject rights for AI processing personal data.	Coverage is strongest where personal data are processed but less complete for non-personal harms, product safety, competition, labour, and broader algorithmic discrimination. Sectoral regulator leadership creates depth but not full horizontal coverage.
Netherlands/EU	Integrated binding risk-and-rights benchmark	EU AI Act risk tiers, GDPR rights, algorithm register, coordinating supervision, impact-assessment practices, and public-sector guidance.	High compliance complexity, cost, and specialist-resource requirements; fragmented implementation remains possible across authorities. Supranational law and mature regulators enable stronger controls than most developing states can immediately replicate.

Why the Regulatory Pathways Differ

First, regulatory purpose matters. India, Kenya, and Malaysia explicitly use AI policy to accelerate innovation, skills, infrastructure, and investment; therefore, they initially favour guidelines, sandboxes, and sectoral governance. Brazil and the Netherlands place greater weight on fundamental rights and high-risk controls, leading to more formal obligations. Indonesia, South Africa, and the Philippines occupy intermediate positions in which data-protection and sectoral institutions carry much of the governance burden.

Second, data-protection maturity affects the ability to regulate AI. Brazil's LGPD, South Africa's POPIA, the Philippines' Data Privacy Act and active National Privacy Commission, Indonesia's PDP Law, and the EU GDPR supply legal concepts that can be extended to AI. However, a mature data-protection statute does not automatically regulate non-personal group harms, safety failures, misinformation, intellectual-property risks, or public-sector procurement.

Third, institutional and market capacity shapes legal ambition. The Netherlands can support registers, impact assessments, specialist supervision, and EU-wide coordination. Developing countries face shortages of auditors, test facilities, local-language datasets, regulatory budgets, and access to proprietary foreign models. Dependence on multinational providers also reduces domestic regulators' access to training information and technical evidence.

Fourth, regional and supranational pressure produces convergence. Malaysia, the Philippines, and Indonesia are influenced by the ASEAN Guide on AI Governance and Ethics, which encourages human-centricity, accountability, privacy, explainability, and internal governance. The Netherlands is legally embedded in the EU AI Act. African states draw on continental digital and AI strategies but retain wide national implementation discretion. These differences explain why similar ethical principles produce different levels of enforceability.

Table 3. Causal Variables Explaining Regulatory Divergence

Causal variable	Observed effect	Implication for developing countries
Dominant policy objective	Innovation-oriented systems prefer flexible guidelines; rights-oriented systems favour binding high-risk obligations.	Use universal minimum rights while phasing in demanding compliance duties.
Maturity of data and administrative law	Existing privacy and public-law institutions can absorb some AI functions.	Build on existing regulators instead of creating an entirely new institution immediately.
Technical and fiscal capacity	Audit, testing, enforcement, and registers require specialist resources.	Calibrate duties to capacity and establish shared testing or accreditation mechanisms.

Dependence on foreign AI providers	Regulators may lack access to training data, model documentation, and cross-border evidence.	Require deployer documentation, contractual audit access, and international cooperation.
Regional/supranational pressure	ASEAN encourages soft convergence; EU law creates binding convergence.	Pursue interoperability without copying resource-intensive institutional designs.
Inequality and legal culture	The same system can distribute risks differently across groups and regions.	Include representativeness, accessibility, and affected-community participation in impact assessment.

Data Governance and Rights

Across the jurisdictions, data-protection law provides the most developed legal entry point, but AI exposes limitations in consent-based and individualised models. Training may rely on scraped or repurposed data; historical datasets may underrepresent local languages, regions, genders, or socio-economic groups; and the influence of deleted data may persist in trained parameters. Publicly accessible data do not become legally unprotected merely because they can be collected at scale. The Philippines provides a useful operational lesson by expressly applying transparency, lawful basis, data minimisation, privacy impact assessment, and data-subject rights to AI training and testing. The Netherlands adds stronger public transparency and risk-monitoring instruments, while Malaysia supplies practical organisational guidance.

The weakness common to developing jurisdictions is limited independent verification. Providers frequently control information about provenance, annotation, model performance, security, and known limitations. Therefore, legal duties must extend beyond privacy notices to dataset documentation, representativeness testing, security controls, provenance records, and regulator access. Ferreira et al. (2022) support this broader relationship between privacy, transparency, and institutional accountability.

Table 4. Data-Governance Risks and Required Controls

Lifecycle stage	Primary risk	Required control
Collection and scraping	Unclear lawful basis, inadequate notice, and extraction of publicly accessible personal data.	Purpose specification, lawful basis, accessible notice, provenance records, and minimisation.
Dataset selection	Historical bias, exclusion, and weak local-language or regional representation.	Representativeness assessment, documentation, bias testing, and affected-group consultation.
Training and fine-tuning	Secondary use, insecure processing, memorisation, and inability to trace influence.	Purpose limitation, security, access control, testing, and records of training and fine-tuning.

Deployment	Function creep, inaccurate outputs, automation bias, and discriminatory impact.	Context-specific validation, human oversight, monitoring, and incident reporting.
Cross-border provision	Different legal protections and limited access to foreign providers.	Contractual audit rights, transfer safeguards, local representative, and regulator cooperation.
Correction and deletion	Data or harmful patterns may persist after a deletion request.	Model-level evaluation, retraining or suppression where feasible, and transparent limitation notices.

Lifecycle Accountability and Transparency

The evidence does not support treating AI itself as the primary bearer of legal responsibility. Although legal-personhood proposals identify genuine doctrinal questions (Novelli, 2022), responsibility is more enforceable when attached to humans and legal entities according to control, knowledge, economic benefit, and capacity to prevent harm. This approach also responds to the responsibility gap identified by Königs, (2022) and the criminal-law uncertainty discussed by (Ma & Zhang, 2024).

Transparency should be differentiated. System-level transparency concerns purpose, model type, data categories, performance, limitations, and responsible parties. Decision-level transparency concerns the principal factors affecting an individual outcome. Regulatory transparency concerns confidential access by supervisors and auditors. Public transparency concerns registers, impact summaries, and incident information. None of these necessarily requires publication of source code or trade secrets, but each requires sufficient information to enable oversight, contestation, and remedy.

Table 5. Allocation of Responsibility Across the AI Lifecycle

Actor	Control and expected duty	Potential responsibility
Model developer	Design, training, testing, technical documentation, foreseeable misuse controls.	Design defects, unsafe performance, bias, inadequate testing, or misleading documentation.
Data provider	Collection, licensing, cleaning, labelling, provenance, and representativeness.	Unlawful, inaccurate, insecure, or systematically unrepresentative data.
Application provider/integrator	Adaptation, interface design, context validation, user information, and safeguards.	Integration failure, unsuitable use context, or inadequate disclosure.
Deployer/organisation	Purpose selection, procurement, impact assessment, monitoring, human review, and remedies.	Harm arising from deployment policy, lack of oversight, or failure to respond.
Professional user	Critical review of outputs and compliance with professional standards.	Automation bias, negligent reliance, or failure to verify consequential decisions.

Infrastructure provider	Security, availability, logging, and contractual cooperation.	Security or service failures within the provider's sphere of control.

The CAPRI-AI Governance Model

The principal scientific contribution is the CAPRI-AI model. It is derived from the finding that effective governance depends on the interaction of legal obligations, rights, lifecycle responsibility, and the capacity to implement them. The model rejects two extremes: unstructured ethical soft law and immediate transplantation of the most demanding developed-country regime. It instead combines five elements that can be operationalised and empirically evaluated.

Table 6. CAPRI-AI Conceptual Governance Model

C Capacity-calibrated implementation	A Accountable lifecycle allocation	P Proportionate risk classification	R Rights- and data-based safeguards	I Iterative institutional learning

Capacity-calibrated implementation means that the legal objective remains constant protection against unacceptable harm but institutional duties are introduced through a realistic sequence. Accountable lifecycle allocation assigns duties to the actors best able to control each risk. Proportionate risk classification differentiates prohibited, high-risk, limited-risk, and minimal-risk uses according to harm, context, scale, reversibility, and affected vulnerability. Rights- and data-based safeguards guarantee lawful processing, non-discrimination, notice, explanation, human review, contestation, and remedy. Iterative institutional learning requires sandboxes, incident reporting, regulatory guidance, periodic review, public registers, and international interoperability.

Table 7. Operational Components and Indicators of CAPRI-AI

Component	Core legal mechanism	Illustrative indicator
Capacity-calibrated implementation	Staged duties, shared audit infrastructure, accredited experts, and sectoral prioritisation.	Ratio of high-risk systems assessed; regulator staffing; audit availability; complaint-processing time.
Accountable lifecycle allocation	Statutory responsibility matrix, procurement clauses, documentation transfer, and joint liability where appropriate.	Completeness of documentation; named responsible entity; contractual audit access.
Proportionate risk classification	Risk tiers based on severity, probability, scale, reversibility, vulnerability, and public-interest context.	Share of systems classified; consistency across sectors; review of classification disputes.

Rights- and data-based safeguards	Lawful basis, impact assessment, data quality, notice, explanation, human review, objection, and remedy.	Rights exercised; reversals after review; bias-test results; remedy effectiveness.
Iterative institutional learning	Sandbox, registry, incident reporting, guidance, periodic evaluation, and cross-border cooperation.	Reported incidents; updated guidance; registry coverage; lessons incorporated into rules.

DISCUSSION

From Descriptive Comparison to Explanatory Comparative Law

The comparison demonstrates that the presence of an AI-specific statute is neither a necessary nor a sufficient measure of governance quality. The Philippines, for example, has operationally specific privacy obligations for AI despite lacking a comprehensive AI Act. Malaysia provides a detailed governance guideline that is useful for organisational implementation but weak in enforceability. Brazil's legislative model is normatively ambitious but faces coordination and compliance challenges. The Netherlands shows how risk tiers, registries, impact assessment, and supervision can interact, but also reveals the administrative intensity of such a system. These differences are best understood as products of policy purpose and institutional capacity rather than as a linear ranking of legal development. This finding refines responsive legal theory. Responsiveness does not mean continuous production of new statutes; it means matching legal instruments to social risk, institutional competence, and mechanisms of participation and correction. A responsive AI regime must therefore be both principled and revisable. Latif et al. (2025) supports adaptive policy, while Wibowo (2025) emphasises a digital-law ecosystem that is transparent, accountable, and sustainable. CAPRI-AI translates these normative claims into institutional design.

Legal Transplantation and Functional Adaptation

The Dutch/EU model should not be copied article by article. Direct transplantation can create obligations that exceed local audit capacity, impose disproportionate costs on startups and public agencies, and produce paper compliance without effective remedies. Rekunenko et al. (2025) similarly identify a gap between regulation and practice in financial-sector comparisons. The appropriate lesson is functional: developing countries can adopt the functions of risk classification, documentation, impact assessment, human review, registry, and remedy while sequencing their institutional form.

Malaysia and the Philippines are therefore particularly relevant to Indonesia. Malaysia demonstrates how a national guideline can align organisations with ASEAN and international standards, clarify governance roles, and support gradual capacity building. Its weakness is the absence of strong enforceability and rights-based remedies. The Philippines demonstrates how an existing privacy regulator can issue specific AI guidance covering training and testing, lawful basis, minimisation, transparency, and accountability. Its

weakness is limited horizontal coverage beyond personal-data processing. Indonesia can combine these lessons: begin with binding rules for high-risk public and sectoral uses, empower existing regulators, and progressively consolidate them into a broader statutory regime.

Interpreting Data, Accountability, and Institutional Findings

Data governance findings confirm that privacy law is necessary but not sufficient. AI creates group-level and inferential harms that individual consent cannot fully address. A rights-based regime must incorporate representativeness, discriminatory impact, local-language performance, security, and the power to contest automated outcomes. This interpretation is consistent with Labadie & Legner (2023), but extends them by locating data duties within a lifecycle and capacity framework.

The responsibility-gap problem should be answered through distributed but non-diffuse accountability. Distributed responsibility recognises that multiple actors control different stages; non-diffuse accountability ensures that an affected person is not forced to identify the entire technical chain before obtaining a remedy. The deployer or institution that determines the purpose of high-risk use should ordinarily provide the first point of accountability, while retaining recourse against developers, data providers, or infrastructure providers. This interpretation is more practical than assigning legal personality to AI and better preserves deterrence and compensation.

Institutional limitations explain why sophisticated rules can fail. Audit obligations require standards, accreditation, secure access to models and logs, and procedures for confidential information. Complaint systems require a clearly competent body and power to suspend harmful systems. Doni et al. (2022) show that governance depends on organisational structures and stakeholder engagement, while (Correia et al., 2025) stress the balance between ethical protection and innovation. CAPRI-AI addresses this balance through risk proportionality and staged capacity development rather than deregulation

Policy Implications for Indonesia

For Indonesia, the most urgent step is not necessarily an immediate omnibus AI Act. A sequenced approach can produce earlier protection and stronger implementation. Existing legal bases should be coordinated through a binding cross-sector instrument for high-risk AI, followed by institutional consolidation as capacity develops. Pancasila values can operate as substantive principles—human dignity, social justice, deliberation, and public interest—while the PDP Law and electronic-systems framework supply enforceable duties. Chen et al. (2024) caution against radical legal interpretations in emerging-economy intellectual-property disputes; the same prudence supports an incremental but rights-protective governance strategy.

Table 8. CAPRI-AI Implementation Roadmap for Indonesia

Phase	Priority Actions	Expected Governance Result
Phase 1: 0–12 months	Issue binding rules for high-risk public-sector and regulated-sector AI; establish a national AI inventory; require notice, impact assessment, human review, incident reporting, and a named accountable institution.	Immediate minimum protection using existing regulators and legal bases.
Phase 2: 1–3 years	Adopt national risk-classification guidance; accredit auditors; create shared testing facilities; standardise procurement clauses and documentation; operate sectoral sandboxes with public reporting.	Consistent implementation and measurable supervisory capacity.
Phase 3: 3–5 years	Enact comprehensive AI legislation; formalise lifecycle responsibility and remedies; create coordinated market surveillance; require public registry for high-impact government algorithms.	Integrated, enforceable, and transparent national AI governance.
Continuous layer	Participatory review, local-language and representativeness testing, international cooperation, ASEAN interoperability, and periodic revision.	Iterative learning and resilience to technological change.

Scientific Contribution and Testable Propositions

The scientific contribution of CAPRI-AI is conceptual, explanatory, and operational. Conceptually, it integrates responsive law, risk-based regulation, rights protection, lifecycle accountability, and institutional capacity. Explanatorily, it predicts that regulatory effectiveness will be highest where obligation intensity is matched by implementation capacity and where affected persons have direct routes to remedy. Operationally, it provides indicators that can be used in empirical research and policy evaluation.

Three propositions follow. Proposition 1: adding high-risk obligations without audit and remedial capacity increases formal compliance but not substantive protection. Proposition 2: lifecycle responsibility reduces accountability gaps more effectively than legal personality for AI. Proposition 3: peer-jurisdiction learning produces more implementable governance than direct transplantation from mature developed-country regimes, provided that minimum rights are not diluted. These propositions distinguish the study from descriptive comparison and create an agenda for future empirical testing.

The study remains normative and document-based. It does not directly measure enforcement, organisational behaviour, regulator experience, or the perspectives of affected communities. The 57-document purposive corpus improves comparative breadth but cannot capture every sectoral instrument or rapidly changing policy. The Netherlands is a functional benchmark, not an economically equivalent comparator. Future research should therefore test CAPRI-AI through interviews, case studies, regulatory data, and sector-specific impact assessments.

This study has three principal limitations. First, its normative and documentary design does not permit direct assessment of how AI rules are enforced in practice or how regulators, developers, deployers, and affected individuals experience those rules. Second, the purposively selected corpus of 57 documents is analytically structured rather than statistically representative and cannot capture every sector-specific or rapidly emerging regulatory instrument. Third, the comparative assessment identifies explanatory patterns rather than statistically established causal relationships. These limitations do not undermine the value of the proposed CAPRI-AI model but define its status as a normative-comparative governance framework that requires subsequent empirical validation.

CONCLUSIONS AND RECOMMENDATIONS

AI-governance challenges in developing countries arise from the interaction of fragmented norms, data risks, diffuse responsibility, weak remedies, and institutional limitations. The comparative analysis suggests that differences in governance pathways are associated with they pursue different policy objectives, possess different data-law and administrative foundations, face unequal technological dependence, and operate under different regional pressures. Brazil and the Netherlands offer stronger risk-and-rights structures; Malaysia and the Philippines offer more transferable ASEAN lessons; India, Kenya, and South Africa demonstrate innovation- and strategy-led pathways; and Indonesia has a valuable but fragmented foundation that requires coordination and enforceability.

The recommended model is CAPRI-AI: Capacity-calibrated implementation, Accountable lifecycle allocation, Proportionate risk classification, Rights- and data-based safeguards, and Iterative institutional learning. Governments should establish universal minimum duties for all AI systems and progressively stricter obligations for prohibited and high-risk uses. They should prioritise impact assessment, documentation, human oversight, accessible complaint and remedy, public-sector transparency, accredited audit capacity, procurement controls, and cross-border cooperation.

For Indonesia, the immediate priority is a binding high-risk governance instrument and national AI inventory coordinated through existing regulators, followed by audit accreditation, shared testing infrastructure, standardised procurement, and eventually comprehensive legislation. This staged approach protects rights without treating institutional capacity as an excuse for inaction and avoids importing a complex foreign regime without the institutions necessary to make it effective.

ADVANCED RESEARCH

Further studies should empirically test the CAPRI-AI propositions through interviews with regulators, developers, deployers, professional users, auditors, civil-society organisations, and affected communities. A comparative AI-governance readiness index could measure legal completeness, data safeguards, lifecycle accountability, audit capacity, remedies, public participation, and cross-border cooperation. Sectoral studies in health, finance, education, employment, biometrics, social assistance, and public procurement are needed to determine whether risk classification and impact assessment produce measurable reductions in harm

ACKNOWLEDGMENT

The authors express appreciation to the academics, regulators, government institutions, international organisations, and publishers whose legal documents, policy materials, books, reports, and scientific literature supported this research. The authors also acknowledge the contribution of Indonesian digital-law scholarship to the formulation of an adaptive and rights-oriented governance framework.

REFERENCES

Alnaim, A. K. (2025). Adaptive zero trust policy management framework in 5G networks. Mathematics, 13(9), 1501.

Arvante, J. Z. Y., Sulistyawan, A. Y., & Riyanto, Y. P. (2025). The Role of Legal Theory in the Era of Digital Globalization: A Perspective of Law Theory as a Tool of Social Engineering. Jurnal Pembangunan Hukum Indonesia, 7(2), 307–324.

Association of Southeast Asian Nations. (2024). ASEAN guide on AI governance and ethics. https://asean.org/wp-content/uploads/2024/02/ASEAN-Guide-on-AI-Governance-and-Ethics_beautified_201223_v2.pdf.

Autoriteit Persoonsgegevens. (2025). AI & algorithmic risks report Netherlands (4th ed.). https://www.autoriteitpersoonsgegevens.nl/en/documents/ai-algorithmic-risks-report-netherlands-arr-february-2025.

Bennett, S. J. (2025). Artificial intelligence and the ethics of navigating ambiguity. Big Data & Society, 12(2), 20539517251347590.

Bourgeois, A., Horrill, T., Mollison, A., Stringer, E., Lambert, L. K., & Stajduhar, K. (2024). Barriers to cancer treatment for people experiencing socioeconomic disadvantage in high-income countries: a scoping review. BMC Health Services Research, 24(1), 670.

Cao, Z., Lai, Z., Bilawal Khaskheli, M., & Wang, L. (2025). The risk of global environmental change to economic sustainability and law: Help from digital technology and governance regulation. Sustainability, 17(15), 7094.

Chattopadhyay, D., & Foster, V. (2025). Distinctive regulatory challenges in developing countries. In Handbook on electricity regulation (pp. 504–533). Edward Elgar Publishing.

Chen, W., Yin, J., Tian, Y., Shang, H., & Li, Y. (2024). Study examining the significant role of intellectual property protection in driving radical technological innovation among national research project teams, employing PLS-SEM and ANN modeling. PloS One, 19(8), e0307026.

Correia, P. M. A. R., Pedro, R. L. D., & Videira, S. (2025). Artificial intelligence in healthcare: Balancing innovation, ethics, and human rights protection. Journal of Digital Technologies and Law, 3(1), 143–180.

de Vries, B. (2023). Individual criminal responsibility for autonomous weapons systems in international criminal law (Vol. 65). Brill.

Department of Communications and Digital Technologies, Republic of South Africa. (2024). South Africa national artificial intelligence policy framework. https://www.dcdt.gov.za/sa-national-ai-policy-framework.html.

Doni, F., Corvino, A., & Bianchi Martini, S. (2022). Corporate governance model, stakeholder engagement and social issues evidence from European oil and gas industry. Social Responsibility Journal, 18(3), 636–662.

Emon, M. M. H. (2026). Navigating the digital labyrinth: Personal data privacy and security at individual and organizational levels. In User-Centric Cybersecurity Implications for Sustainable Digital Transformation (pp. 257–288). IGI Global Scientific Publishing.

European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

Ferreira, A., Bandeira, A. M., Santos, C., Ferreira, I., Tomé, B., Costa, A. J., Joaquim, C., Góis, C., Curi, D., & Meira, D. (2022). Can online transparency improve accountability? The case of Portuguese private social solidarity institutions. Sustainability, 14(3), 1632.

Fischer, A. (2023). Data sovereignty and e-governance: The legal implications of national laws on digital government systems. Legal Studies in Digital Age, 2(4), 1–12.

Gardi, B., & Eddine, B. A. S. (2023). Cyber security and personal data protection in the digital age: Challenges, impacts, and urgency of global collaboration. Bulletin of Science, Technology and Society, 2(3), 58–63.

Giest, S. N., & Klievink, B. (2024). More than a digital system: how AI is changing the role of bureaucrats in different organizational contexts. Public Management Review, 26(2), 379–398.

Government of the Netherlands. (2024). Government-wide vision on generative AI of the Netherlands. https://www.government.nl/documents/2024/01/17/government-wide-vision-on-generative-ai-of-the-netherlands.

Government of the Netherlands. (n.d.). The algorithm register of the Dutch government. https://algoritmes.overheid.nl/en.

Heo, S., Sohn, W., Park, S., & Lee, D. K. (2024). Multi-hazard assessment for flood and Landslide risk in Kalimantan and Sumatra: Implications for Nusantara, Indonesia's new capital. Heliyon, 10(18).

IndiaAI. (2025). India AI governance guidelines: Empowering ethical and responsible AI. https://indiaai.gov.in/article/india-ai-governance-guidelines-empowering-ethical-and-responsible-ai.

Jun, S., Park, H., Kim, U.-J., Choi, E. J., Lee, H. A., Park, B., Lee, S. Y., Jee, S. H., & Park, H. (2023). Cancer risk based on alcohol consumption levels: a comprehensive systematic review and meta-analysis. Epidemiology and Health, 45, e2023092.

KANG, S. L., & HAVERCROFT, J. (2025). Constructing Normative Foundations. The Oxford Handbook of Norms Research in International Relations, 397.

Kementerian Komunikasi dan Informatika Republik Indonesia. (2023). Surat Edaran Menteri Komunikasi dan Informatika Republik Indonesia Nomor 9 Tahun 2023 tentang Etika Kecerdasan Artifisial. https://jdih.komdigi.go.id/produk_hukum/view/id/883.

Kenya Ministry of Information, Communications and the Digital Economy, Republic of Kenya. (2025). Kenya artificial intelligence strategy 2025–2030. https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf

Königs, P. (2022). Artificial intelligence and responsibility gaps: What is the problem? Ethics and Information Technology, 24(3), 36.

Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. Journal of Information Technology, 38(1), 16–44.

Latif, M., Kurniawan, D. W., & Pertiwi, T. W. (2025). Transformation of Digital Legislation Policy as the Basis for Adaptive Regulation and Harmonisation of Global Human Rights. The Virtual International Conference on Economics, Law and Humanities, 4(1), 290–298.

Lim, E. C. N., & Lim, C. E. D. (2025). Polycentric AI governance: A multi-stakeholder approach to distributed responsibility and ethical technology management. International Journal of Advanced AI Applications, 1(4), 77–97.

Lovell, J. J. (2023). Legal Aspects of Artificial Intelligence Personhood: Exploring the Possibility of Granting Legal Personhood to Advanced Ai Systems and the Implications for Liability, Rights and Responsibilities. Rights and Responsibilities.(May 10, 2023).

Ma, Y., & Zhang, X. (2024). Scientific uncertainty and the challenges of applying criminal law: Lessons from China's COVID-19 response. Heliyon, 10(14).

Ministry of Science, Technology and Innovation, Malaysia. (2024). The national guidelines on AI governance and ethics. https://mastic.mosti.gov.my/publication/the-national-guidelines-on-ai-governance-ethics.

National Privacy Commission, Republic of the Philippines. (2024). NPC Advisory No. 2024-04: Guidelines on the application of the Data Privacy Act to artificial intelligence systems processing personal data. https://privacy.gov.ph/wp-content/uploads/2025/02/Advisory-2024.12.19-Guidelines-on-Artificial-Intelligence-w-SGD.pdf.

Novelli, C. (2022). AI and legal personhood: a theoretical survey.

Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: what it is and how it works. Ai & Society, 39(4), 1871–1882.

Plantinga, P., Dlamini, N., Pienaar, G., Nkosi, M., Davids, Y. D., Okem, A., & Dlamini, S. (2023). The governance of eParticipation: towards a rights-based approach. 2023 IST-Africa Conference (IST-Africa), 1–16.

Raimi, L. (2026). First-mover advantage in AI adoption in higher education: a critical discourse analysis of social policy, inequality, and institutional governance. International Journal of Sociology and Social Policy, 1–23.

Rekunenko, I., Koldovskyi, A., Babenko, K., & Subačienė, R. (2025). The impact of financial regulation on financial control efficiency: A comparative analysis of economies. Accounting and Financial Control., 6(1), 13–24.

Republic of Indonesia. (2019). Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/122030/pp-no-71-tahun-2019.

Republic of Indonesia. (2022). Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022.

Republic of Indonesia. (2024). Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024.

Senado Federal do Brasil. (2023). Projeto de Lei No. 2338/2023: Dispõe sobre o uso da inteligência artificial. https://www25.senado.leg.br/web/atividade/materias/-/materia/157233.

Wen, Z., & Tong, D. (2023). Analysis of the legal subject status of artificial intelligence. Beijing L. Rev., 14, 74.