IIAR JOURNALS

Innovating Knowledge. Advancing Research.

IIAR Journal of Governance and Public Administration

Vol 1, No 1, 2026

Governing Artificial Intelligence in Developing States: A Theoretical Analysis of Regulatory Capacity, Policy Transfer and Institutional Design for National AI Strategies in Africa

NWOGBOJI Emmanuel Usulor[1], OGAH Sunday Ogbo[2]

[1,2] Veristzon Global Research Lab

ABSTRACT

African governments are adopting national artificial intelligence (AI) strategies and drafting AI laws, often modelled on European, American or Chinese templates, in states where regulatory capacity for far simpler technologies is thin. Existing scholarship asks whether such documents exist, whether they reflect African values and whether states are ready to implement them, but says little about how a rule, once written, comes to be observed and enforced. This article seeks to explain that gap and to identify institutional designs suited to capacity-constrained states. It adopts a conceptual, theory-building design based on an integrative review of 30 peer-reviewed journal articles published between 2023 and 2026 and one continental policy instrument, combined with typology construction, proposition derivation and an illustrative case. Drawing on regulatory-state and regulatory-capacity scholarship, policy-transfer and diffusion theory, comparative research on AI governance regimes and recent work on African AI strategies, it distinguishes three governance functions: rule-making, monitoring and enforcement. The central finding is that imported frameworks are rule-heavy while African states are weakest in monitoring and enforcement, so that adoption produces regulation on paper: formally binding obligations that are rarely observed, selectively enforced and often most burdensome for domestic firms. The article assesses regional regulatory pooling, procurement as a governance lever, sectoral regulation and the use of data-protection authorities as AI regulators, and derives seven testable propositions on when each works, on the political economy of regulating AI while courting AI investment, and on the relationship between national strategies and the African Union's 2024 Continental AI Strategy. Nigeria's national AI strategy process anchors the analysis, with Rwanda, Kenya, Egypt, Mauritius and South Africa as comparators. Theoretically, the article treats regulatory capacity as a function-specific property; practically, it recommends a capacity-first review sequence in which every new obligation is paired with an institution able to monitor it.

Keywords: AI governance; regulatory capacity; policy transfer; national AI strategy; institutional design

Governing Artificial Intelligence in Developing States: A Theoretical Analysis of Regulatory Capacity, Policy Transfer and Institutional Design for National AI Strategies in Africa

1. INTRODUCTION

In April 2024, Nigeria's Federal Ministry of Communications, Innovation and Digital Economy closed a four-day workshop in Abuja at which more than 120 researchers, practitioners, firms and civil society groups worked towards a national AI strategy. The organisations listed as supporting the exercise included Google, Meta and Microsoft, alongside UNESCO, UNDP and the country's own technology agencies. A draft strategy was released in August 2024. Weeks earlier, in July 2024, the African Union Executive Council had endorsed a Continental Artificial Intelligence Strategy that asks member states to adopt national strategies, review their data protection, consumer and competition laws, and build "innovative and agile regulatory instruments" (African Union, 2024).

Across the continent, ministries are producing strategies, councils, ethics charters and draft bills at speed. Scholarship has largely asked whether these documents exist, whether they reflect African values, and whether states are ready to implement them. Those are fair questions. They are not the decisive one.

This article argues that the central problem of governing AI in African states is not a shortage of rules but a mismatch between the governance functions that imported frameworks emphasise and the functions that capacity-constrained states can perform. The templates now circulating, above all the European Union's AI Act but also American voluntarism and Chinese administrative control, are elaborate in rule-making and quietly presuppose monitoring and enforcement. African regulators are weakest precisely there. Transplanting rule-heavy frameworks into such settings yields regulation on paper: obligations that are formally binding, rarely observed and selectively enforced.

The purpose of the article is to build a theory of that mismatch and to derive from it an institutional-design framework for states that must govern AI with limited capacity. Three questions organise the inquiry. Which governance functions do the circulating AI frameworks emphasise, and which do they presuppose? Under what conditions can capacity-constrained states govern AI through regional pooling, procurement, sectoral supervision or data-protection authorities rather than through a new horizontal regulator? And how does the political economy of courting AI investment shape the distance between rules and practice? Nigeria anchors the analysis, with Rwanda, Kenya, Egypt, Mauritius and South Africa as comparators. The focus throughout is the state as regulator of AI markets, not the state as user of AI in its own administration.

2. LITERATURE REVIEW

2.1 CONCEPTUAL REVIEW

AI governance is used here in the broad sense developed by Veale et al. (2023): the set of modalities through which the development and use of AI are steered, ranging from ethics councils and technical standards to contracts, licensing and domestic laws with extraterritorial reach. A national AI strategy is one such modality. Papyshev and Yarime (2023), analysing 31 strategies, show that every strategy mixes three state roles, development, control and promotion, in varying proportions; strategies are therefore statements of industrial ambition as well as of regulatory intent.

Regulatory capacity is the concept on which the article turns, and it is contested. Queiroz Cunha and Lodge (2025) show that development-oriented regulatory reform has been dominated by a "low-discretion" doctrine, which treats capacity as the ability to apply clear rules predictably, and that disappointment with it has revived a more discretionary understanding in which capacity means the ability to exercise judgement under uncertainty. The article disaggregates capacity by function. Rule-making is the production of binding or guiding norms. Monitoring is the generation of reliable information about who deploys which systems, for what purposes and with what effects. Enforcement is

© IIARJournal. All rights reserved.

the imposition of costs on non-compliance. A state may be strong in one and weak in the others.

Policy transfer denotes the movement of rules, institutions and ideas from one jurisdiction to another, whether by deliberate borrowing, external pressure or market-driven diffusion. In AI the leading case is the supposed "Brussels effect" of the EU AI Act, whose reach recent work treats with scepticism (Almada & Radu, 2024; Crum, 2025). Finally, regulation on paper names the outcome this article theorises: an adopted rule set whose formal obligations exceed the domestic capacity to verify and sanction them.

2.2 THEORETICAL REVIEW

Four theoretical traditions inform the argument. The first is regulatory-state theory. Giandomenico Majone's regulatory state governs through rule-making by specialised agencies, a model that development reform widely exported, and Queiroz Cunha and Lodge (2025) show that the doctrine attached to it equated capacity with rule-bound predictability. AI unsettles that equation. Judge et al. (2025) argue that systems built through deep learning cannot be specified or audited against explicit rules in the way that aircraft or nuclear plants can, and that effective oversight will require consolidated authority, licensing, mandated disclosure, formal verification and a capacity for rapid intervention. Read from Lagos or Kigali, that list is less a programme than an inventory of what is missing.

The second is policy-transfer theory. David Dolowitz and David Marsh distinguished transfers that are uninformed, incomplete or inappropriate to their destination, and AI regulation risks all three at once. Anu Bradford's "Brussels effect" predicts that EU rules spread through market incentives; Charles Sabel and Jonathan Zeitlin's experimentalist governance predicts instead iterative, recursive rule-making with local revision. Crum (2025) finds the second account fits the AI Act better. This article uses transfer theory to ask a narrower question: which parts of a regulatory model travel with its text, and which stay behind.

The third is institutional theory, specifically the idea associated with John Meyer and Brian Rowan that organisations adopt formal structures to secure legitimacy with external audiences while decoupling them from practice. The fourth is the political economy of regulation, from George Stigler's theory of capture onward, which recent work extends to AI by showing that large technology firms have become central actors in policy processes (Khanal et al., 2025) and that even the EU regulates partly to build a competitive market (Paul, 2024). Combined, these traditions suggest that regulation on paper is not simply a failure of implementation. It can be a rational response by governments addressing two audiences at once.

2.3 EMPIRICAL REVIEW

Comparative research on AI regimes provides the template side of the problem. Papyshev and Yarime (2023) find that EU members emphasise control while the United States and United Kingdom favour promotion. Hine (2024) characterises American governance as voluntary and industry-led, gradually moving towards legislation, and Chinese governance as increasingly centralised. Tallberg et al. (2023) set out an agenda for explaining such regimes, and Ulnicane (2025) observes that the first international initiatives on generative AI were dominated by a small group of developed countries and framed technocratically as risk management.

Evidence on transfer is increasingly sceptical. Almada and Radu (2024) argue that because the AI Act is built on EU product-safety law, its diffusion would export a framework offering limited protection to fundamental rights. Crum (2025) concludes that the Act's procedural character, reliance on self-certification and split oversight make wholesale copying difficult, and Ebers (2025) warns non-EU legislators against following it blindly. The most instructive Global South evidence comes from data protection: Gadoni Canaan (2023) shows that Brazil's replication of the GDPR stimulated a domestic market for privacy-enhancing technologies whose gains were largely captured by Western firms.

Research on African AI policy is more mixed than its volume suggests. Plantinga et al. (2024), reviewing policy and legislation in twelve countries, warn against treating AI as exceptional and urge learning from existing capabilities such as model management in banking, transparency rules for public-private partnerships and electronic transactions law; they also flag consultant dependence and the loss of

© IIARJournal. All rights reserved.

institutional memory across electoral cycles. Ayana et al. (2024), assessing ten sub-Saharan states, find institutional capacity the weakest of their governance indicators. Diallo et al. (2025) show that global readiness indices misread African progress, and Effoduh et al. (2024) argue for context-specific data governance rather than wholesale adoption of external frameworks. Farhad (2025) proposes that Global South states build AI governance capacity through incremental, locally grounded cycles of assessment and policy action. On enforcement specifically, Raji et al. (2025) and Faturoti and Juma (2025) document the powers and constraints of African data-protection authorities.

What this literature lacks is a middle. It is strong at the level of strategy documents and values, and increasingly strong on readiness. It is thin on the mechanics by which a rule, once written, comes to be observed and enforced. Readiness indices reward the existence of documents; decolonial critiques interrogate their content. Neither tells us whether a lending app's credit-scoring model in Lagos will ever be examined by anyone with the authority to stop it. That is the gap this article addresses.

3. MATERIALS AND METHODS

The study uses a conceptual, theory-building design. It is non-empirical in the sense that it collects no primary data; it involves no human participants, so ethics approval was not required.

The population of sources is the peer-reviewed journal literature on AI governance, regulatory capacity, policy transfer and African AI and data-protection policy. Sources were identified through keyword searches of scholarly indexes and publisher platforms combining terms such as "AI governance", "regulatory capacity", "policy transfer" and "Africa", and by citation chaining. Inclusion criteria were peer-reviewed journal articles published from 2023 to 2026, including online-first versions; direct relevance to at least one of the constructs; and English language. Preprints, conference papers, books and chapters, editorials, items that could not be verified and retracted items were excluded. One primary policy document, the African Union's (2024) Continental AI Strategy, was included because the argument concerns its design directly. Descriptive facts about national instruments, such as Nigeria's draft strategy and its 2023 data protection statute, are drawn from the cited literature and publicly available official sources.

Each reference was checked against its DOI landing page, publisher record, or a bibliographic-index or institutional-repository record for authors, title, journal, volume, issue, pages or article number, and retraction or correction status. Candidates that could not be confirmed were dropped. The final corpus comprises 30 journal articles and one primary document.

The analysis proceeded in three stages. An integrative thematic synthesis grouped findings around capacity, templates, transfer and African practice; the typology was then constructed by asking, for each template and design option, which function it emphasises and which it presupposes. Propositions were derived from the interaction of these functions with political-economic incentives. Nigeria and five African comparators serve as an illustrative, theory-probing case: they were chosen because they are well documented in the corpus and vary in institutional arrangements, not because they represent the continent.

The bases of judgement are transparency of selection criteria, an audit trail of verification, triangulation across the regulatory, transfer and African-policy literatures, explicit boundary conditions and propositions stated so that they can be falsified. A conceptual design cannot establish causal effects, and its illustrations depend on what the literature records.

The key constructs are formal stringency of AI rules, monitoring capacity, enforcement capacity and observed regulatory effect. Future tests could operationalise them respectively through coded legal texts, regulators' technical staffing and information sources, budgets and sanctioning powers, and published sanctions, complaint-handling times and court decisions.

AI usage disclosure: A generative AI assistant (Claude, Anthropic) was used to support literature searching, reference verification against bibliographic records, drafting and language editing. The author(s) reviewed, revised and verified all content, checked every reference against its publisher or index record, and take full responsibility for the manuscript.

© IIARJournal. All rights reserved.

4. RESULTS AND DISCUSSION

4.1 RESULTS

4.1.1 Writing Rules, Watching Markets, Imposing Costs

Rule-making is the cheapest governance function to import. Legal text travels easily; a statute can be drafted by a small team or a donor-funded consultant within months, and borrowing a template carries apparent legitimacy. Strategies and bills therefore multiply faster than agencies.

Monitoring is the function on which the argument turns. It requires notification duties that firms honour, technical staff able to test systems, complaint channels that citizens use, and routine data from regulated entities. AI makes each harder than it is for conventional products. Systems are updated continuously, often delivered by providers with no local presence, and embedded in services whose users cannot see the model. The opacity Judge et al. (2025) identify is first a monitoring problem.

Enforcement depends on monitoring but is not reducible to it. It also requires legal powers, procedural capacity to survive challenge, and political autonomy to act against firms that governments may be courting. Where monitoring is weak, enforcement becomes episodic and selective. The regulator acts against what it happens to see: what is domestic, visible and politically unprotected.

The functions interact in ways that the language of "implementation gaps" obscures. Rules without monitoring do not lie dormant. They create discretion, because officials can choose when to invoke them, and in low-accountability settings discretion can become a source of rents: a licensing duty that no one checks systematically can still be used to extract payments from those who are checked. Rule-heaviness also distributes burdens perversely. Domestic start-ups that register, document and seek approval bear compliance costs that foreign providers serving the same market through global platforms may never face, an outcome that echoes Gadoni Canaan's (2023) finding about transplanted data protection law.

Each major template embeds an assumption about monitoring that does not travel with its text (Table 1). Under the EU AI Act, compliance for high-risk systems is established largely through conformity assessment, provider self-assessment, notified bodies and harmonised standards, with national market surveillance authorities required to have permanently available staff expert in AI, data protection, cybersecurity and fundamental rights (Novelli et al., 2025). Gstrein et al. (2024) conclude that its success depends on enforcement and cooperation, and Laux et al. (2024) argue that it overstates what regulation can achieve by equating trustworthiness with acceptable risk. Without Europe's standards bodies, accredited auditors and funded surveillance authorities, the Act becomes a list of duties no one can verify. The American template presupposes dense ex post accountability through litigation, consumer-protection agencies and an investigative press; voluntary frameworks function there because other institutions do the monitoring (Hine, 2024). The Chinese template presupposes an administrative state with deep reach into platforms, and is the least transferable to states without comparable administrative penetration.

Table 1. AI governance templates and the capacity they presuppose

Template	Rule-making emphasis	Monitoring and enforcement assumed	Likely result in a low-capacity state
EU AI Act	Detailed risk-tier duties	Notified bodies, standards, staffed surveillance authorities, fines	Duties verified only by self-declaration
United States	Guidance, voluntary frameworks	Litigation, consumer agencies, press, courts	Effectively self-regulation
China	Targeted administrative measures	Filing with inspection; strong state power over firms	Unchecked registration; selective or rent-seeking use

Regulation on paper deserves a concession. Paper rules signal alignment to trading partners, give courts and civil society textual hooks for later litigation, and may anchor enforcement once capacity grows. The objection is to sequencing and proportion, not to rules as such. A state that adopts a full horizontal regime before it can monitor any part of it spends scarce

© IIARJournal. All rights reserved.

political and administrative capital on the least constrained function.

4.1.2 Design Options Under Capacity Constraint

If monitoring is the binding constraint, design should begin by asking where monitoring capacity already exists or can be cheaply generated. Four options follow, and they do not deserve equal confidence.

Regional pooling is the option most often recommended and, I suspect, the most overrated. The Continental Strategy promotes "regionally integrated governance approaches" (African Union, 2024), and at the global level Roberts et al. (2024) prefer strengthening coordination among existing institutions over creating new centralised ones. Technical evaluation, incident databases and standards are expensive and largely non-rival, so pooling has a real logic. But it is far easier for rule-making and information-sharing than for enforcement, which states guard as an attribute of sovereignty. Farhad (2025) is right that regional cooperation can support national capacity but not replace it.

Procurement is the most underrated option. Governments and state-owned enterprises are major and visible buyers of digital systems, and procurement converts regulatory aims into contract terms. A ministry buying a credit-assessment system can make documentation, testing, audit access and incident reporting conditions of award, monitor them through contract management, and enforce them through payment and termination. Veale et al. (2023) identify contracts as a distinct modality of AI governance; Effoduh et al. (2024) call for foreign AI systems to be procured transparently with attention to accountability and knowledge transfer; the Continental Strategy calls for standards on public procurement of AI (African Union, 2024); and Gadoni Canaan (2023) suggests procurement as a vehicle for local-content requirements. The limits are obvious. Procurement reaches only public deployments, and procurement systems are themselves frequent sites of capture.

Sectoral regulation is the most immediately practicable option. Central banks, telecommunications regulators and securities commissions already hold supervisory relationships, receive routine data and possess enforcement powers. Adding AI-specific expectations, for example on credit-scoring models, uses monitoring channels that already work; Plantinga et al. (2024) identify model management in banking as such a capability. Roberts et al. (2023) defend the United Kingdom's sector-led approach while warning that pressure to weaken checks in the name of innovation could undermine it, and Gikay (2024) argues that incremental sectoral regulation adapts better to evolving risks than a horizontal classification. The cost is unevenness: strong supervisors protect citizens in their domains while weak ones, often in health, education or labour, leave large areas exposed.

Data-protection authorities are, for most African states, the default. Raji et al. (2025) find that all twenty English-language African data protection laws they examined require a dedicated authority, and that most provide for administrative, financial and criminal sanctions and require controllers to register or notify. Many AI harms run through personal data processing. Novelli et al. (2025) note that EU member states may assign AI Act functions to such bodies, and Mazur (2026) shows that even in Europe the division of labour between data protection authorities and AI-specific enforcers remains poorly coordinated. Yet African authorities are young and often thinly resourced.

Regulatory sandboxes cut across these options and are best understood as monitoring devices for regulators. Buocz et al. (2023) find that the AI Act's sandbox provisions leave unresolved questions of competence, equal treatment, liability and consent; Taeihagh (2025) presents sandboxes as instruments of iterative learning, while Plantinga et al. (2024) warn that they can obscure relationships and invite capture. In a low-capacity state, a sandbox's principal value is that it obliges firms to reveal information the regulator could not otherwise obtain.

4.1.3 Propositions

The following propositions state the conditions under which the diagnosis and design options should hold, framed comparatively so that they can be tested.

> **Proposition 1.** Holding the formal stringency of AI rules constant, the gap between formal obligation and observed regulatory effect will be larger where an adopted framework assigns monitoring to institutions that do not exist

© IIARJournal. All rights reserved.

domestically, such as notified bodies, accredited auditors and specialised market surveillance authorities.

States with near-identical texts should diverge according to their monitoring infrastructure, and the divergence should be greatest for obligations whose verification is technical (documentation, testing, data quality) rather than observable (prohibitions on visible uses).

Proposition 2. Regional regulatory pooling will improve AI governance outcomes when it is confined to monitoring-intensive but sovereignty-light tasks, including shared technical evaluation, common standards and incident registers, and will fail when it extends to enforcement; its effectiveness will increase with the presence of a funded anchor institution and with member-state contributions that are actually paid.

States gain from pooled testing and shared registers without surrendering control, so cooperation is self-enforcing. Enforcement pooling asks states to accept that a regional body may penalise firms they are trying to attract. The data protection precedent, in which regional instruments preceded national enforcement, suggests that harmonised text alone does little.

Proposition 3. Procurement-based AI governance will be effective where public bodies account for a substantial share of high-stakes AI deployment and where procurement is digitised, published and subject to independent review; it will be ineffective where procurement is captured, and its reach will be bounded by the public share of deployment.

Procurement solves the monitoring problem by making disclosure a condition of payment and the enforcement problem by replacing prosecution with contract remedies. Both advantages vanish if awards are opaque or politically directed. Strong procurement governance may also push high-risk applications towards private markets it cannot reach.

Proposition 4. Sectoral AI regulation will outperform a horizontal AI statute in sectors where supervisors already hold routine reporting relationships with regulated entities, such as banking and telecommunications, and will underperform in sectors with weak supervisors, producing uneven protection that mirrors the prior distribution of regulatory capacity.

This concedes the strongest argument for horizontal regulation, namely coverage. A single statute at least names every high-risk domain. But naming is not monitoring. Unevenness is the price of effectiveness and should be stated openly.

Proposition 5. Assigning AI oversight to an existing data-protection authority will be effective when that authority has budgetary independence, an established practice of complaint handling and audit, and a caseload in which AI harms arise from personal data processing; adding AI mandates to an under-resourced authority will dilute its core data-protection enforcement.

Discriminatory scoring, automated denial of services and profiling pass through personal data; safety failures in industrial systems and market concentration do not. The dilution claim is the important qualification. A new mandate without new money is a reallocation, and the first casualty will be the routine complaint handling on which the authority's legitimacy rests.

Proposition 6. In states actively courting AI investment, governments will favour rule-making that signals alignment with external templates while tolerating weak monitoring, because visible rules attract partners and weak enforcement reassures investors; the gap between rule and practice will narrow where domestic actors, including courts, data-protection authorities, civil society organisations and domestic firms facing asymmetric compliance burdens, can independently trigger enforcement.

This is the political economy of regulation on paper. Khanal et al. (2025) show that large technology firms use their centrality in AI policy processes largely in their own interests. Paul (2024) demonstrates that the EU's risk-based framework served to fashion a competitive common market and an image of trustworthiness as much as to control risk, and

© IIARJournal. All rights reserved.

Mügge (2024) finds that European "AI sovereignty" has prioritised jurisdictional independence and an AI-race logic while neglecting effects on people outside the Union. Capacity-constrained states regulating partly to attract investment should do the same with greater intensity and less monitoring. The decoupling is less hypocrisy than a rational answer to two audiences.

> **Proposition 7.** Continental AI frameworks will raise national governance capacity only when they specify a division of labour between continental, regional and national tiers and carry dedicated resources; frameworks that call in general terms for harmonisation will produce convergent national strategies and divergent implementation.

The Continental Strategy endorses multi-tiered governance, harmonisation, regional advisory boards, sandboxes and procurement standards, and asks the AU Commission to prepare a five-year implementation plan (African Union, 2024). As direction it is sensible; as design it leaves open which functions sit at which tier, and so will mainly supply vocabulary for national documents, useful for rule-making and nearly irrelevant to monitoring.

4.2 DISCUSSION

4.2.1 Nigeria and Its Comparators

Nigeria shows the diagnosis with unusual clarity because it is rich in rule-making and in institutions, and thin in monitoring. Responsibility for AI policy sits with the Federal Ministry of Communications, Innovation and Digital Economy and with the National Information Technology Development Agency (NITDA). Ayana et al. (2024) identify NITDA as the body guiding AI regulation and rate Nigeria as aware of, but not yet responsive to, the demands of AI sovereignty. The August 2024 draft strategy organised its ambitions around five pillars, including responsible and ethical AI and an AI governance framework; according to the OECD's policy observatory, a finalised strategy for 2025–2029 was published in September 2025. Several bills proposing a dedicated AI regulator have been introduced in the National Assembly.

The Nigeria Data Protection Act, signed in June 2023, created the Nigeria Data Protection Commission and gave data subjects a right not to be subject to decisions based solely on automated processing that produce significant effects. On paper, Nigeria already has an AI-relevant regulator with sanctioning powers. In practice, Faturoti and Juma (2025) find a commission whose funding depends on contributions from other regulators, whose independence is exposed, and whose technical and audit capacity remains limited. The record also points in a more hopeful direction. Abusive digital lending apps, which harvested borrowers' contacts and shamed defaulters, eventually drew coordinated action from Nigerian regulators, including delisting and privacy sanctions. Enforcement succeeded where a market was domestic, visible and politically unprotected, as the framework predicts.

A standalone AI commission, as some bills propose, would add a rule-maker without adding monitoring capacity, and would compete for mandate with NITDA, the data protection commission and sector regulators. The stronger path combines existing assets: a data protection commission with independent funding for harms that run through personal data; sector supervisors, the central bank above all, extending model governance to credit scoring and fraud systems; and NITDA's established role in clearing federal information technology projects as a procurement gate for public-sector AI. That global technology firms sponsored the 2024 workshop is not evidence of capture, but it illustrates the dual audience of Proposition 6.

The comparators sharpen the picture. Rwanda, rated the most responsive of ten states by Ayana et al. (2024), routes AI oversight through its multi-sector utilities regulator, grafting AI onto an existing supervisory body. Kenya shows how a data-protection authority can grow: Faturoti and Juma (2025) describe an office with parliamentary funding, a transparent appointment process and regional offices, which has audited and penalised digital lenders. Diallo et al. (2025) record that Kenya's president directed the drafting of AI legislation in 2023, and Kenya has since adopted a national AI strategy for 2025–2030. Egypt, which formed a National Council for AI in 2019 and adopted a charter for responsible AI in 2023 (Diallo et al., 2025), illustrates a council-led model in which soft-law commitments precede enforceable obligations. Mauritius published one of Africa's first strategies in

© IIARJournal. All rights reserved.

2018, yet Diallo et al. (2025) note gaps in its data protection law, including unclear enforcement powers. South Africa has strong data protection regulation but, in the assessment of Ayana et al. (2024), no dedicated AI governance institution. Early strategy, strong statute and strong council are each weak proxies for monitoring capacity.

4.2.2 Relation to Prior Studies

The framework agrees with Plantinga et al. (2024) and Farhad (2025) that African states should build from existing capabilities and proceed incrementally, and it agrees with Almada and Radu (2024) and Crum (2025) that the AI Act will not diffuse cleanly. It extends that work in two directions. Where Ayana et al. (2024) and Diallo et al. (2025) treat institutional capacity or readiness as a single dimension, this article disaggregates it by function and predicts that strategies and statutes will outrun monitoring. And it locates the failure of transfer on the receiving side, in the absent verification layer.

It departs from prior work in three places. Judge et al. (2025) prescribe consolidated authority and licensing; for capacity-constrained states this article argues the opposite sequence, distributing AI duties across bodies that already monitor something. It is more doubtful than the Continental Strategy (African Union, 2024) about regional governance, confining pooling to information. And against the view that a comprehensive statute offers the best protection, it treats horizontal coverage without monitoring as largely nominal, closer to Gikay's (2024) incrementalism.

4.2.3 A Capacity-First Review Sequence

The framework yields a sequence for drafters, to be applied before adoption and at each review. The first step attaches to every proposed obligation a named monitor, its information source and the cost of obtaining it; obligations without a named monitor should be deferred, converted into guidance or redesigned so that compliance is self-revealing. The second exhausts existing institutions, mapping sector supervisors, the data-protection authority and the procurement clearance body against identified risks before creating new agencies. The third prefers information-generating instruments, such as registers of public-sector AI systems, incident-reporting clauses in procurement contracts and sandbox participation conditioned on disclosure. The fourth pools testing and standards while keeping enforcement national. The fifth protects the budgets of bodies receiving AI mandates and adds sunset and review clauses so that obligations are revisited as capacity grows.

4.2.4 Limitations and Future Research

The argument treats monitoring and enforcement capacity as variables without offering a validated measure of either. Its illustrations come mainly from anglophone states, reflecting the literature, and francophone and lusophone traditions may distribute the three functions differently.

Each proposition is nonetheless testable. Proposition 1 could be examined by coding the formal stringency of AI and data protection laws and comparing it with enforcement records drawn from annual reports, published sanctions and court decisions. Propositions 2 and 7 suit process tracing as the AU implementation plan unfolds. Proposition 3 could be tested by comparing audit terms in published AI procurement contracts across states with different procurement transparency; Proposition 4 by comparing AI supervision in finance and health within Nigeria or Kenya; Proposition 5 by before-and-after analysis of complaint-handling times and sanction rates in authorities that acquire AI mandates; and Proposition 6 through interviews and document analysis of who drafted strategies, who funded consultations and how investment promotion was weighed against oversight.

5. CONCLUSION AND RECOMMENDATIONS

African states have not been slow to write AI rules. If anything, they have been quick to write rules whose operation depends on institutions they do not yet have. The rule-making–monitoring–enforcement distinction shows why this matters: imported frameworks concentrate ambition in the function that is cheapest to transfer and leave unaddressed the function that determines whether any of it bites. Regulation on paper is the result, and its costs fall unevenly, often on domestic firms and citizens rather than on the global providers whose systems carry the greatest consequence. The design options examined here are not a menu of equals. Procurement and sectoral supervision work with monitoring channels

© IIARJournal. All rights reserved.

that exist; data-protection authorities can carry more if funded and independent; regional pooling is valuable for information and much weaker for sanction.

Ministries drafting or revising AI strategies, Nigeria's included, should ensure that no obligation enters a draft without a named monitor, and should create new agencies only for functions existing bodies cannot absorb.

Legislatures should resist standalone AI commissions that add rule-makers without monitors, and should instead give data-protection authorities statutory funding lines independent of other agencies, together with sunset and review clauses on AI obligations.

Sector supervisors and data-protection authorities should extend existing model governance and complaint handling to AI, beginning with credit scoring and digital lending, where monitoring channels and enforcement precedents already exist. Procurement clearance bodies should make documentation, audit access and incident reporting conditions of award for public-sector AI.

The African Union and regional economic communities should use the Continental Strategy's implementation plan to allocate functions between tiers, pooling technical evaluation and standards while leaving enforcement national. Donors and technology partners should fund monitoring capacity rather than further drafting. Researchers should test the seven propositions against enforcement records.

6. CONTRIBUTION TO EXISTING KNOWLEDGE

Theoretically, the article treats regulatory capacity as a function-specific property rather than a single attribute of states, showing how a mismatch between rule-making, monitoring and enforcement produces regulation on paper. It joins policy-transfer theory to this distinction by identifying what travels with a regulatory text and what stays behind, and it draws on institutional and political-economy theory to explain why governments courting investment may rationally prefer visible rules to effective monitoring.

For the African and developing-state literature, it supplies the missing middle between strategy-level analysis and readiness assessment, specifying the mechanisms by which a written AI rule becomes observed and enforced, and it offers seven propositions that can be tested against enforcement records, procurement contracts and process-traced continental implementation.

For policy, it ranks design options rather than listing them, favouring procurement and sectoral supervision, conditioning reliance on data-protection authorities on their funding and independence, and confining regional pooling to information. The capacity-first review sequence gives ministries, legislators and continental bodies a practical test for every proposed AI obligation.

7. REFERENCES

African Union. (2024). *Continental artificial intelligence strategy: Harnessing AI for Africa's development and prosperity*. African Union Commission. https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf

Almada, M., & Radu, A. (2024). The Brussels side-effect: How the AI Act can reduce the global reach of EU policy. *German Law Journal*, *25*(4), 646–663. https://doi.org/10.1017/glj.2023.108

Ayana, G., Dese, K., Nemomssa, H. D., Habtamu, B., Mellado, B., Badu, K., Yamba, E., Faye, S. L., Ondua, M., Nsagha, D., Nkweteyim, D., & Kong, J. D. (2024). Decolonizing global AI governance: Assessment of the state of decolonized AI governance in Sub-Saharan Africa. *Royal Society Open Science*, *11*(8), Article 231994. https://doi.org/10.1098/rsos.231994

Buocz, T., Pfotenhauer, S., & Eisenberger, I. (2023). Regulatory sandboxes in the AI Act: Reconciling innovation and safety? *Law, Innovation and Technology*, *15*(2), 357–389. https://doi.org/10.1080/17579961.2023.2245678

Crum, B. (2025). Brussels effect or experimentalism? The EU AI Act and global standard-setting. *Internet Policy Review*, *14*(3). https://doi.org/10.14763/2025.3.2032

Diallo, K., Smith, J., Okolo, C. T., Nyamwaya, D., Kgomo, J., & Ngamita, R. (2025). Case studies of AI policy development in Africa. *Data & Policy*, *7*, Article e15. https://doi.org/10.1017/dap.2024.71

Ebers, M. (2025). Truly risk-based regulation of artificial intelligence: How to implement the EU's AI Act. *European Journal of Risk Regulation*, *16*(2), 684–703. https://doi.org/10.1017/err.2024.78

© IIARJournal. All rights reserved.

Effoduh, J. O., Akpudo, U. E., & Kong, J. D. (2024). Toward a trustworthy and inclusive data governance policy for the use of artificial intelligence in Africa. *Data & Policy*, *6*, Article e34. https://doi.org/10.1017/dap.2024.26

Farhad, S. (2025). Passengers in flight: AI governance capacity in the Global South. *Digital Society*, *4*(2), Article 39. https://doi.org/10.1007/s44206-025-00195-6

Faturoti, B., & Juma, I. (2025). Enforcing data privacy in Kenya and Nigeria: Towards an African approach to regulatory practice. *International Review of Law, Computers & Technology*. Advance online publication. https://doi.org/10.1080/13600869.2025.2506918

Gadoni Canaan, R. (2023). The effects on local innovation arising from replicating the GDPR into the Brazilian General Data Protection Law. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1686

Gikay, A. A. (2024). Risks, innovation, and adaptability in the UK's incrementalism versus the European Union's comprehensive artificial intelligence regulation. *International Journal of Law and Information Technology*, *32*, Article eaae013. https://doi.org/10.1093/ijlit/eaae013

Gstrein, O. J., Haleem, N., & Zwitter, A. (2024). General-purpose AI regulation and the European Union AI Act. *Internet Policy Review*, *13*(3). https://doi.org/10.14763/2024.3.1790

Hine, E. (2024). Governing Silicon Valley and Shenzhen: Assessing a new era of artificial intelligence governance in the United States and China. *Digital Society*, *3*(3), Article 50. https://doi.org/10.1007/s44206-024-00138-7

Judge, B., Nitzberg, M., & Russell, S. (2025). When code isn't law: Rethinking regulation for artificial intelligence. *Policy and Society*, *44*(1), 85–97. https://doi.org/10.1093/polsoc/puae020

Khanal, S., Zhang, H., & Taeihagh, A. (2025). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society*, *44*(1), 52–69. https://doi.org/10.1093/polsoc/puae012

Laux, J., Wachter, S., & Mittelstadt, B. (2024). Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk. *Regulation & Governance*, *18*(1), 3–32. https://doi.org/10.1111/rego.12512

Mazur, J. (2026). The role of data protection authorities in the enforcement regime concerning the general-purpose artificial intelligence in the AI Act. *Journal of Law, Market & Innovation*, *5*(2), 312–336. https://doi.org/10.13135/2785-7867/13848

Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? *Journal of European Public Policy*, *31*(8), 2200–2225. https://doi.org/10.1080/13501763.2024.2318475

Novelli, C., Hacker, P., Morley, J., Trondal, J., & Floridi, L. (2025). A robust governance for the AI Act: AI Office, AI Board, scientific panel, and national authorities. *European Journal of Risk Regulation*, *16*(2), 566–590. https://doi.org/10.1017/err.2024.57

Papyshev, G., & Yarime, M. (2023). The state's role in governing artificial intelligence: Development, control, and promotion through national strategies. *Policy Design and Practice*, *6*(1), 79–102. https://doi.org/10.1080/25741292.2022.2162252

Paul, R. (2024). European artificial intelligence "trusted throughout the world": Risk-based regulation and the fashioning of a competitive common AI market. *Regulation & Governance*, *18*(4), 1065–1082. https://doi.org/10.1111/rego.12563

Plantinga, P., Shilongo, K., Mudongo, O., Umubyeyi, A., Gastrow, M., & Razzano, G. (2024). Responsible artificial intelligence in Africa: Towards policy learning. *Data & Policy*, *6*, Article e72. https://doi.org/10.1017/dap.2024.60

Queiroz Cunha, B., & Lodge, M. (2025). Contesting regulatory capacity: Exploring doctrines in the regulatory state. *Public Administration and Development*. Advance online publication. https://doi.org/10.1002/pad.2108

Raji, M., Wilder, D., Ugwuoke, V., & Bashir, M. (2025). An assessment of the enforcement mechanisms in African data protection laws. *African Journal on Privacy & Data Protection*, *2*(1), 1–40. https://doi.org/10.29053/ajpdp.v2i1.0002

Roberts, H., Babuta, A., Morley, J., Thomas, C., Taddeo, M., & Floridi, L. (2023). Artificial intelligence regulation in the United Kingdom: A path to good governance and global leadership? *Internet Policy Review*, *12*(2). https://doi.org/10.14763/2023.2.1709

Roberts, H., Hine, E., Taddeo, M., & Floridi, L. (2024). Global AI governance: Barriers and pathways forward. *International Affairs*, *100*(3), 1275–1286. https://doi.org/10.1093/ia/iiae073

© IIARJournal. All rights reserved.

Taeihagh, A. (2025). Governance of generative AI. *Policy and Society*, *44*(1), 1–22. https://doi.org/10.1093/polsoc/puaf001

Tallberg, J., Erman, E., Furendal, M., Geith, J., Klamberg, M., & Lundgren, M. (2023). The global governance of artificial intelligence: Next steps for empirical and normative research. *International Studies Review*, *25*(3), Article viad040. https://doi.org/10.1093/isr/viad040

Ulnicane, I. (2025). Governance fix? Power and politics in controversies about governing generative AI. *Policy and Society*, *44*(1), 70–84. https://doi.org/10.1093/polsoc/puae022

Veale, M., Matus, K., & Gorwa, R. (2023). AI and global governance: Modalities, rationales, tensions. *Annual Review of Law and Social Science*, *19*, 255–275. https://doi.org/10.1146/annurev-lawsocsci-020223-040749

© IIARJournal. All rights reserved.