Regulating Artificial Intelligence in Africa: A Comparative Legal Analysis of Regulatory Frameworks and Governance Approaches

Chinyelu Ifeoma Emechebe[1*], Azubuike Nzubechukwu Aniedu[2], Sandra Chioma Nwokoye[3]

[1]Faculty of Law, Nnamdi Azikiwe University, Awka, Nigeria

[2,3]Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria

***Corresponding Author**

DOI: https://doi.org/10.47772/IJRISS.2026.101000147

Received: 13 October 2026; Accepted: 18 October 2026; Published: 30 October 2026

ABSTRACT

Artificial intelligence is being deployed across African economies faster than the law has adapted to govern it. This article undertakes a doctrinal and comparative analysis of the legal frameworks through which the African Union and five national jurisdictions (Nigeria, Kenya, South Africa, Rwanda and Egypt) regulate AI, using the EU AI Act, the Council of Europe Framework Convention and the OECD and UNESCO instruments as reference points. Its objectives are to map the approaches adopted, assess how they address the core legal problems raised by AI, and determine how much they borrow from external models. It finds that African AI governance is strategy-rich and statute-poor: every jurisdiction studied has an AI strategy or policy, but none had a comprehensive AI statute confirmed in force by October 2026. Data protection law serves as the de facto law of AI, and recent decisions, including the Kenyan High Court's Worldcoin judgment and the Nigerian tribunal ruling upholding a US$220 million penalty against Meta, show it can be enforced vigorously. Liability, algorithmic discrimination and the explainability of automated decisions are nonetheless addressed only incidentally, and draft legislation in Nigeria and Kenya transplants the EU's risk-based architecture without the institutional infrastructure that supports it. The article also identifies an emerging problem of AI-generated falsehoods within legal and governmental institutions, illustrated by South African court decisions on fictitious citations and the withdrawal of the country's draft national AI policy. It proposes a staged, capacity-sensitive legislative approach and specific reforms on liability, discrimination, administrative justice, collective data interests and the verification of AI-generated material. These findings suggest that effective AI governance in Africa will depend less on the breadth of new statutes than on obligations that existing institutions can credibly enforce.

Keywords: artificial intelligence regulation, AI governance, data protection, comparative law, legal transplants

INTRODUCTION

Artificial intelligence has moved from the margins of African policy discourse to its centre in a remarkably short period. Credit-scoring algorithms now decide who receives mobile loans in Nairobi and Lagos; facial recognition systems have been procured for urban surveillance in several capitals; and generative models are being used, sometimes carelessly, in the drafting of court submissions. Each deployment raises questions the existing body of law was not designed to answer. Who bears liability when an automated decision causes harm? Can a person contest a decision whose reasoning even its developer cannot fully reconstruct? And does a data protection statute modelled on a European template offer meaningful protection in a society where much personal data is collected informally and enforcement agencies are thinly resourced?

The global regulatory response has been uneven but increasingly assertive. The European Union adopted Regulation (EU) 2024/1689, the Artificial Intelligence Act, which entered into force on 1 August 2024 and

established the first comprehensive, horizontal, risk-based statute for AI. The Council of Europe opened its Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law for signature in September 2024. Alongside these binding instruments sit influential soft-law texts, notably the OECD Recommendation on Artificial Intelligence (OECD, 2024) and the UNESCO Recommendation on the Ethics of Artificial Intelligence (UNESCO, 2021).

Africa has not been a bystander. The African Union Executive Council endorsed a Continental Artificial Intelligence Strategy in July 2024, and the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) finally entered into force in June 2023, almost a decade after its adoption. At national level, a growing number of states have published AI strategies or policies, and more than thirty-five now have comprehensive data protection legislation. Yet very few African jurisdictions have enacted AI-specific legislation. The continent's legal response to AI therefore rests, for now, on a layered and somewhat improvised architecture: general data protection statutes, consumer and competition law, constitutional rights, sectoral regulation, and a body of non-binding strategies whose legal force is uncertain.

This article addresses a mismatch between the pace and character of AI adoption in Africa and the legal frameworks available to govern it. Three features sharpen the problem. First, most African AI governance instruments are policy documents rather than law, so the rights and duties they describe are frequently unenforceable. Second, where binding rules exist, they are often transplanted from external models, chiefly the EU's General Data Protection Regulation, without sustained inquiry into whether those models fit local institutional capacity, legal pluralism, or economic conditions. Third, the scholarly literature remains weighted toward ethical principles and the European and North American experience, leaving comparatively little doctrinal analysis of how African statutes, courts, and regulators actually address AI-related harms.

The general objective is to analyse, from a comparative perspective, the legal and regulatory frameworks through which African states and regional bodies govern artificial intelligence, and to propose reforms that close the identified gaps. Four research questions follow from this objective:

1. What legal and governance approaches to AI have African states and continental and regional bodies adopted, and how are binding and non-binding instruments distributed across them?

2. How do these frameworks address the core legal problems raised by AI, namely liability, non-discrimination, transparency and explainability, data protection and automated decision-making, and institutional accountability?

3. To what extent do African instruments transplant, adapt or depart from external models such as the EU AI Act, the GDPR, the OECD principles and the UNESCO Recommendation?

4. What legal gaps remain, and what reforms would make AI governance in Africa more effective, enforceable and contextually grounded?

Theoretical Orientation

Three bodies of theory frame the analysis. The first is the theory of risk-based regulation, which holds that regulatory effort should be calibrated to the probability and severity of harm rather than spread uniformly across an activity. The EU AI Act is its most prominent application to AI, sorting systems into prohibited, high-risk, limited-risk and minimal-risk categories. Critics have long cautioned that risk-based regimes depend on technocratic judgements about what counts as risk, and that those judgements can quietly exclude harms that fall unevenly on marginalised groups (Smuha, 2021).

The second is the theory of legal transplants. Watson (1974) argued that borrowing rules across legal systems is common and largely unproblematic, whereas Legrand (1997) insisted that a rule cannot truly travel because its meaning is bound up with the legal culture that produced it. For African AI governance, this debate is not

academic. Bradford's (2020) account of the "Brussels Effect" explains why EU rules diffuse globally through market pressure, and data protection in Africa offers abundant evidence of that diffusion (Makulilo, 2016). Whether a transplanted AI regime can function where enforcement agencies are under-resourced, where courts are slow, and where customary norms govern much of social life is precisely the question the Brussels Effect leaves open.

The third is the decolonial and relational critique of AI governance. Birhane (2020) describes the uncritical import of AI systems and their governing assumptions into African contexts as a form of "algorithmic colonisation", while Mhlambi (2020) and Gwagwa, Kazim and Hilliard (2022) propose Ubuntu, a relational ethic that locates personhood in community, as an alternative foundation to the individualist premises of Western data protection. These perspectives sharpen the comparative inquiry: they ask not only whether African frameworks resemble foreign ones, but whether resemblance is desirable.

Continental and regional instruments

At the continental level, the most significant binding instrument remains the Malabo Convention of 2014, which entered into force in June 2023. Its data protection chapter establishes principles of consent, purpose limitation and data subject rights, and it restricts decisions based solely on automated processing that produce legal effects. Its low ratification count and the absence of a strong supervisory mechanism limit its practical weight (Abdulrauf, 2021). In 2021, the African Commission on Human and Peoples' Rights adopted Resolution 473, calling on states to ensure AI technologies conform to the African Charter on Human and Peoples' Rights. The Resolution is not binding, but it anchors AI governance in the continent's regional human rights system.

The Continental AI Strategy, endorsed by the African Union Executive Council at its 45th Ordinary Session in July 2024, is the principal policy framework. It is development-oriented: it treats AI primarily as a tool for achieving Agenda 2063 and the Sustainable Development Goals, and it asks member states to adopt national strategies, build capacity and develop governance arrangements in step with one another. It does not impose regulatory obligations. A political signal of continental alignment followed at the Global AI Summit on Africa in Kigali in April 2025, where forty-nine African countries, the African Union and Smart Africa endorsed an Africa Declaration on Artificial Intelligence.

Regional economic communities have been more active on data protection than on AI. The ECOWAS Supplementary Act A/SA.1/01/10 on Personal Data Protection (2010) and the SADC Model Law on Data Protection (2013) both pre-date the current wave of AI policy, but they provided templates that shaped many national statutes, and in the case of ECOWAS the Supplementary Act is binding on member states.

National frameworks in the selected jurisdictions

Nigeria. The Nigeria Data Protection Act 2023 established the Nigeria Data Protection Commission and introduced a right not to be subject to a decision based solely on automated processing, subject to exceptions. On AI specifically, the Federal Ministry of Communications, Innovation and Digital Economy published a National Artificial Intelligence Strategy on 19 September 2025, framed as a living document covering 2025 to 2029. The National Assembly has introduced several AI bills, including the National Artificial Intelligence Commission (Establishment) Bill (SB 731, February 2025) and a Nigerian Artificial Intelligence Bill (HB 2567, October 2025) (Digital Policy Alert, n.d.-a). The most consequential vehicle, the National Digital Economy and E-Governance Bill, would reportedly confer AI governance functions on the National Information Technology Development Agency (NITDA), require impact assessments for higher-risk systems in areas such as finance and public administration, and allow fines of up to ₦10 million or 2 per cent of an AI provider's annual Nigerian revenue (BusinessDay, 2026; Mobile World Live, 2026). Presidential assent was announced as imminent in November 2025 and passage was again targeted for March 2026 (AllAfrica, 2025; Techpoint Africa, 2026).

Kenya. Kenya's Data Protection Act 2019 is the operative binding law for most AI-related processing. The National AI Strategy 2025–2030 was launched on 27 March 2025 (Techweez, 2026). The Artificial Intelligence

Bill, 2026, sponsored by Senator Karen Nyamu and introduced to the Senate in February 2026, proposes a risk-based regime, an independent Office of the Artificial Intelligence Commissioner with powers of inspection and administrative fines, and an obligation on high-risk providers and deployers to comply with the Data Protection Act, including by conducting impact assessments (Bowmans, 2026). Because it touches county functions, the Bill must pass both Houses. Kenya also published a draft Artificial Intelligence and Other Emerging Technologies Policy for public participation in 2026 (Capital FM, 2026).

South Africa. South Africa relies on the Constitution, the Protection of Personal Information Act 2013 (POPIA), whose section 71 restricts decisions based solely on automated processing, and on sectoral regulation. After a National AI Policy Framework in August 2024, Cabinet approved a Draft National AI Policy, which was gazetted for comment on 10 April 2026. The draft proposed an unusually elaborate institutional architecture, including a National AI Commission, an AI Ethics Board, an AI Regulatory Authority, an AI Ombudsperson, a National AI Safety Institute and an AI Insurance Superfund to compensate victims where liability is uncertain (Cliffe Dekker Hofmeyr, 2026). On 26 April 2026 the Minister of Communications and Digital Technologies withdrew it, after confirming that its reference list contained fictitious sources, most plausibly AI-generated citations included without verification (SAnews, 2026). An expert panel was appointed, and a revised draft is expected to go to Cabinet by November 2026 and to be released for comment in January 2027 (Reuters, 2026).

Rwanda. Rwanda adopted a National Artificial Intelligence Policy in 2023, one of the earliest on the continent. It is paired with Law No. 058/2021 on the protection of personal data and privacy, which established a supervisory function within the National Cyber Security Authority. Rwanda's approach is strategy-led and state-coordinated, with an emphasis on positioning the country as a hub for responsible AI development and on public-sector adoption.

Egypt. Egypt's National Council for Artificial Intelligence issued the second edition of the National AI Strategy (2025–2030) in January 2025, building on a first strategy of 2021 and the Egyptian Charter for Responsible AI of 2023 (Digital Policy Alert, n.d.-b). The strategy identifies the enactment of an AI law and a Centre for Responsible AI as its main governance mechanisms; a draft law with risk-based classification has been discussed with stakeholders but was not publicly available at the time of writing (Legal 500, 2026; Chambers and Partners, 2025). Binding obligations meanwhile flow from the Personal Data Protection Law No. 151 of 2020 and sectoral legislation.

Global reference models

Four external instruments serve as comparators. The EU AI Act, Regulation (EU) 2024/1689, is the only comprehensive horizontal AI statute among them. Its prohibitions applied from February 2025 and its obligations for general-purpose AI models from August 2025. In 2026, however, the EU adopted a Digital Omnibus amendment that deferred the high-risk obligations for stand-alone systems from 2 August 2026 to 2 December 2027, and for AI embedded in regulated products to 2 August 2028 (K&L Gates, 2026). The deferral is instructive in itself: even the most institutionally resourced regulator in the world has found the high-risk regime difficult to operationalise on schedule.

The Council of Europe Framework Convention is the first binding international treaty on AI, though its obligations are framed at a level of generality that leaves wide discretion to parties. The OECD Recommendation on AI and the UNESCO Recommendation on the Ethics of AI are non-binding, but both have been influential in Africa. The UNESCO Readiness Assessment Methodology, in particular, has been applied in several African states and has shaped the vocabulary of their strategies.

Comparative Overview

The most striking comparative finding is structural. Every jurisdiction studied has a national AI strategy or policy, either adopted or in draft, and every one has a general data protection statute. None, as at October 2026,

has a comprehensive AI statute confirmed in force. Africa's AI governance is therefore a matter of strategy above and data protection below, with a legislative middle tier that is still being built. Table 1 sets out the position.

Table 1: AI governance instruments in the selected jurisdictions, as at October 2026

Jurisdiction	AI strategy or policy	Dedicated AI legislation	Data protection statute	Right concerning solely automated decisions	Proposed or designated AI oversight body
Nigeria	National AI Strategy 2025–2029 (Sept 2025)	National Digital Economy and E-Governance Bill and other AI bills; yet to be enacted	Nigeria Data Protection Act 2023	Yes, with exceptions	NITDA (under the Bill); National AI Commission proposed (SB 731)
Kenya	National AI Strategy 2025–2030 (Mar 2025); draft AI and Emerging Technologies Policy (2026)	Artificial Intelligence Bill, 2026 (Senate)	Data Protection Act 2019	Yes, with exceptions	Office of the AI Commissioner proposed
South Africa	AI Policy Framework (Aug 2024); Draft National AI Policy withdrawn Apr 2026, revision due 2027	None	POPIA 2013	Yes (s 71), with exceptions	Multiple bodies proposed in withdrawn draft
Rwanda	National AI Policy (2023)	None	Law No. 058/2021	Yes, with exceptions	Existing ICT and data protection institutions
Egypt	Second National AI Strategy 2025–2030 (Jan 2025)	Draft AI law, not public	Law No. 151 of 2020	Limited	Centre for Responsible AI proposed
African Union	Continental AI Strategy (July 2024)	None	Malabo Convention (in force 2023)	Yes (Convention)	No continental regulator
European Union (comparator)	Coordinated Plan on AI	AI Act 2024/1689, as amended 2026	GDPR 2016/679	Yes (GDPR art 22)	AI Office and national authorities

Three observations follow from the table. First, the right concerning solely automated decisions, which originates in the European data protection tradition, is now present in almost every African statute examined; it is the clearest instance of transplantation in the field. Second, the draft legislation in Nigeria and Kenya adopts risk-based classification, impact assessment and a dedicated supervisory office, which are the signature features of the EU AI Act. Third, the institutional design of the proposed regulators varies considerably, from a single consolidated digital regulator in Nigeria to the multiplicity of bodies envisaged in the withdrawn South African draft.

Data protection law as the de facto law of AI

In the absence of AI statutes, data protection law carries most of the regulatory weight, and the cases show that it can carry a good deal. The clearest example is the Kenyan litigation against Worldcoin. On 5 May 2025, the High Court (Aburili J), on a judicial review application brought by the Katiba Institute and other civil society organisations (Katiba Institute v Worldcoin Foundation, 2025), quashed the decision to collect iris and facial

images through the Worldcoin "Orb", prohibited further collection without a lawful data protection impact assessment, and ordered deletion of all biometric data unlawfully collected, under the supervision of the Data Protection Commissioner (Katiba Institute v Worldcoin Foundation, 2025). The Court found breaches of the impact assessment requirement in section 31 of the Data Protection Act 2019 and held that consent obtained through inducement by cryptocurrency was not valid. The Data Protection Commissioner confirmed deletion on 20 January 2026 (People Daily, 2026). Two doctrinal points stand out. The decision treats the impact assessment as a condition of lawful processing, not a formality. And its analysis of consent recognises that economic vulnerability can vitiate apparent agreement, a point with obvious significance for AI services offered in low-income markets.

A second line of authority comes from Nigeria, where consumer and competition law has been used to discipline data practices. On 25 April 2025, the Competition and Consumer Protection Tribunal upheld the US$220 million penalty imposed by the Federal Competition and Consumer Protection Commission on Meta Platforms and WhatsApp, following a joint investigation with the Nigeria Data Protection Commission into privacy policies and consumer data practices (Meta Platforms Inc v Federal Competition and Consumer Protection Commission, 2025). The Tribunal held that the Commission acted within its mandate in matters touching on data protection and privacy. The decision does not concern AI as such, but it matters for AI governance because it confirms that regulatory overlap can be productive: a competition and consumer authority, acting alongside a data protection authority, can reach the data-driven business models on which AI services depend.

The limits of the data protection route are equally clear. Data protection law is triggered only by the processing of personal data, and many AI harms arise elsewhere: in the design of a model trained on aggregated or synthetic data, in the safety of an autonomous system, or in the use of AI outputs to make decisions about groups rather than identified individuals. The right not to be subject to solely automated decisions is also easily circumvented, because a nominal human reviewer takes a decision outside the "solely automated" category, and the exceptions for contractual necessity and explicit consent are broad. Data protection law is therefore a necessary but partial foundation.

Liability for AI-caused harm

None of the jurisdictions studied has enacted a liability rule specific to AI. Claims would therefore proceed under general principles of delict or tort, product liability where it exists, and contract. Each presents difficulties. Fault-based liability requires a claimant to prove that a defendant fell below a standard of care, but the opacity of complex models makes it hard to identify which act in a long chain of development and deployment caused the harm, and who performed it. Strict product liability, where available, raises the threshold question of whether software, or a continuously updated AI service, is a "product" at all. The consumer protection statutes in Nigeria - the Federal Competition and Consumer Protection Act 2018, Kenya - the Consumer Protection Act 2012) and South Africa - the Consumer Protection Act 2008, whose section 61 imposes strict liability for harm caused by unsafe goods, provide partial routes, but none was drafted with AI in view.

The proposals under discussion respond in different ways. The Kenyan Bill relies chiefly on administrative enforcement through the AI Commissioner rather than on new civil remedies. The withdrawn South African draft took a more innovative route, proposing an AI Insurance Superfund to compensate victims where liability cannot be clearly allocated. That proposal deserves to survive the withdrawal. It recognises that the central problem for victims is often not the absence of a liable party but the cost and difficulty of identifying one, and it borrows from no-fault compensation schemes familiar in road accident and workplace injury law. The EU, by contrast, withdrew its proposed AI Liability Directive in 2025, leaving the field to its revised Product Liability Directive. African legislators therefore cannot simply follow Brussels on this question, because Brussels has not settled it.

Non-discrimination and equality

The constitutions of Kenya (article 27) and South Africa (section 9) contain strong equality guarantees that apply horizontally in appropriate cases, and South Africa's Promotion of Equality and Prevention of Unfair

Discrimination Act 2000 provides a specialised forum in the Equality Courts. In principle, a person disadvantaged by a biased credit-scoring or recruitment algorithm could invoke these provisions. In practice, three obstacles intervene. Algorithmic discrimination is usually indirect, emerging from correlations in training data rather than explicit use of a protected characteristic, which places a heavy evidentiary burden on claimants. Victims rarely know an algorithm was involved. And the data needed to prove disparate impact is held by the deployer. Neither the Nigerian nor the Kenyan draft legislation yet addresses these evidentiary asymmetries directly, for instance through a reversal of the burden of proof once a prima facie case is shown, or through a statutory right of access to the information needed to test a system for bias.

Transparency, explainability and due process

The demand for transparency is expressed in every strategy examined, but it has been translated into enforceable rights mainly through the data protection provisions on automated decision-making. Where the state uses AI, administrative law offers an additional and underused route. Section 33 of the South African Constitution and the Promotion of Administrative Justice Act 2000 guarantee lawful, reasonable and procedurally fair administrative action and a right to written reasons; article 47 of the Kenyan Constitution and the Fair Administrative Action Act 2015 are to similar effect. A decision taken by or with the help of an algorithm remains administrative action, and the duty to give reasons does not disappear because the reasoning is computational. Read this way, existing administrative law already imposes a meaningful explainability requirement on public-sector AI. The difficulty is that it has scarcely been litigated in this context, and the content of an adequate "reason" for a machine-assisted decision remains undefined.

AI in the administration of justice

The courts themselves have become a site of AI governance. In *Mavundla v MEC: Department of Co-operative Government and Traditional Affairs KwaZulu-Natal* [2025] ZAKZPHC 2, the Pietermaritzburg High Court found that a legal team had submitted non-existent case authorities, most likely produced by a generative AI tool, and referred the matter to the Legal Practice Council (Michalsons, 2025). In *Northbound Processing (Pty) Ltd v South African Diamond and Precious Metals Regulator (Gauteng High Court, Case No. 2025-072038, 30 June 2025)*, the Court again referred practitioners to the regulator, even though the fictitious citations had not been relied upon in oral argument and responsibility was promptly accepted, holding that admonishment alone would not be an adequate response (ENSafrica, 2025). The rule emerging from these judgments is in substance a professional duty of verification: a practitioner who uses AI remains personally responsible for every authority placed before the court.

The withdrawal of South Africa's Draft National AI Policy in April 2026 extends the same lesson to the executive. A policy intended to govern AI was itself compromised by unverified AI-generated references, and the Minister acknowledged the absence of any disclosure that AI had been used in its preparation (Reuters, 2026). The episode is more than an embarrassment. It shows that the duty of verification recognised by the courts has no settled counterpart in public administration, where AI-assisted drafting of policy, regulations and official decisions is presumably widespread and largely undisclosed.

Institutional design and the transplantation question

The draft laws in Nigeria and Kenya borrow the architecture of the EU AI Act with some fidelity, including risk tiers, impact assessments, sandboxes and an enforcement authority. This is not objectionable in itself; regulatory convergence lowers compliance costs for firms operating across markets and can ease cross-border data flows. The difficulty lies in what the transplant leaves behind. The EU regime depends on an infrastructure of harmonised technical standards, notified conformity assessment bodies, national market surveillance authorities and a central AI Office. That infrastructure took years to build and, as the 2026 deferral shows, is still not ready to support the high-risk obligations. A risk-based statute enacted without equivalent capacity risks becoming what Legrand (1997) might call a rule without its culture: formally present, practically inert.

The Nigerian Bill's consolidation of AI functions within NITDA reflects a pragmatic preference for building on an existing agency rather than creating a new one, though it raises questions of coordination with the NDPC, the

Central Bank and sectoral regulators. The withdrawn South African draft illustrates the opposite tendency: an ambitious set of new institutions proposed before questions of funding and overlap had been resolved. Kenya's proposed AI Commissioner lies between the two. A further concern is the size of penalties. A ceiling of ₦10 million, roughly US$7,000, would be negligible to a large multinational, although the alternative of 2 per cent of Nigerian revenue is more serious. By comparison, the Meta proceedings show that Nigerian regulators can already impose very substantial penalties under existing consumer and competition legislation.

Legal pluralism and the limits of the individual-rights model

Finally, the frameworks examined share an assumption inherited from their European models: that the primary unit of protection is the identifiable individual, whose personal data and personal decisions are at stake. Many AI harms in African contexts are collective. Agricultural advisory systems, credit models built on community-level mobile data, and language technologies trained on indigenous-language corpora affect groups, sometimes communities governed in part by customary law. The Malabo Convention and the national data protection statutes have little to say about collective data rights or community consent. The relational ethics proposed by Mhlambi (2020) and Gwagwa, Kazim and Hilliard (2022) are often presented as philosophical alternatives, but they point to a concrete legislative gap: the absence of any mechanism through which communities, as distinct from individuals, can assert interests in data about them or in the systems built from it.

FINDINGS AND RECOMMENDATIONS

The analysis supports five principal findings. The first four respond to the research questions; the fifth emerged from the material itself.

First, African AI governance is strategy-rich and statute-poor. Every jurisdiction examined has articulated national ambitions for AI, and the African Union has supplied a continental framework, yet binding AI-specific legislation remains at the bill stage. Repeated announcements of imminent enactment, as in Nigeria, coexist with slow legislative progress, suggesting the bottleneck is not the political will to announce regulation but the capacity and consensus needed to complete it.

Second, data protection law functions as the de facto law of AI, and it is more effective than often assumed. The Worldcoin judgment in Kenya and the Meta proceedings in Nigeria show courts and regulators willing to impose demanding requirements and substantial penalties on powerful technology firms. The limitation lies in scope rather than strength: data protection does not reach harms that arise without processing personal data, and its individual-rights model fits collective harms poorly.

The third is that the core legal problems of AI (liability, algorithmic discrimination and the explainability of automated decisions) are addressed only incidentally. Existing constitutional, administrative, consumer and equality law offers potential remedies, but they are untested in the AI context, and the evidentiary burdens they impose on claimants are severe.

The fourth is that the emerging legislative models are heavily transplanted. The Nigerian and Kenyan drafts reproduce the architecture of the EU AI Act, yet the EU itself deferred its high-risk obligations in 2026 because the supporting infrastructure was not ready. Transplanting the architecture without the infrastructure risks producing statutes that are formally comprehensive but practically unenforceable.

The fifth finding, which the research design did not anticipate, concerns the use of AI by legal and governmental institutions themselves. The *Mavundla* and *Northbound* judgments and the withdrawal of South Africa's draft policy show that AI-generated hallucinated content has already compromised court submissions and a national policy instrument. A professional duty of verification has been recognised for legal practitioners, but no equivalent rule governs AI-assisted drafting by public bodies.

Recommendations

The following reforms are proposed. They are directed principally at national legislators and regulators, with

some addressed to the African Union and regional economic communities.

1. **Legislate in stages, beginning with what existing institutions can enforce.** Rather than enacting a comprehensive risk-based statute in a single step, legislators should first place on a statutory footing a short list of prohibited practices and a small set of clearly defined high-risk uses, notably in credit, employment, public benefits, biometric identification and law enforcement. Obligations for those uses can be enforced by existing data protection, consumer and sectoral regulators. The scope can be widened as capacity grows.

2. **Strengthen the data protection foundation rather than bypassing it.** Amendments should close the "nominal human review" loophole by requiring that human involvement in an automated decision be meaningful, extend impact assessment duties expressly to high-risk AI systems, and give data protection authorities the budgets their expanded role demands.

3. **Adopt a compensation mechanism for AI-caused harm.** The no-fault fund proposed in the withdrawn South African draft should be retained and studied for adoption elsewhere. Alongside it, legislators should consider a rebuttable presumption of causation where a deployer fails to comply with documentation or logging obligations, and should clarify that software and AI services fall within the scope of product liability provisions.

4. **Ease the evidentiary burden in discrimination claims.** Equality legislation should provide for a shift of the burden of proof once a claimant shows a prima facie case of disparate impact, and should give claimants, or a regulator acting on their behalf, a right of access to the information needed to audit a system for bias.

5. **Make administrative law work for public-sector AI.** Governments should publish registers of algorithmic systems used in public decision-making, and legislation or guidance should specify what an adequate statement of reasons requires when a decision is made with algorithmic assistance.

6. **Codify a duty of verification and disclosure for AI use in law and government.** Rules of court and professional conduct rules should expressly require practitioners to verify AI-generated material and, where required by the court, to disclose its use. An equivalent duty should apply to the preparation of legislation, policy and official decisions, so that AI-assisted drafting is disclosed and every source is checked before publication.

7. **Recognise collective data interests.** Legislators should explore mechanisms for community consent and benefit-sharing where AI systems are trained on data relating to identifiable communities, including indigenous-language data, drawing on customary governance structures where appropriate.

8. **Coordinate regionally to compensate for limited national capacity.** The African Union and regional economic communities should move from strategy to shared infrastructure: model legislation, a common list of high-risk uses, mutual recognition of conformity assessments, and pooled technical expertise for audit and testing. The ECOWAS data protection framework offers a precedent for binding regional rules.

9. **Build the evidence base.** Regulators should be required to report publicly on enforcement activity relating to AI, and research funders should support empirical evaluation of whether the rules adopted actually change practice.

CONCLUSION

This article set out to analyse, in comparative perspective, how African states and regional institutions govern artificial intelligence through law. Its central argument is that Africa's legal response to AI has so far been built from the top and the bottom but not the middle. At the top sit strategies, continental and national, that articulate ambition and principle but create no enforceable rights. At the bottom sit data protection, consumer, constitutional and administrative law, which were not designed for AI but which courts and regulators have

begun to apply to it with some vigour, as the Worldcoin judgment in Kenya and the Meta proceedings in Nigeria demonstrate. The middle tier of AI-specific legislation is now being drafted, and the drafts lean heavily on the European model.

The field is moving quickly. Bills in Nigeria and Kenya may be enacted, and South Africa's revised policy is expected in 2027, so several of the positions described here will change. The underlying questions are more durable: how to make rights enforceable where institutions are stretched, how far to borrow and where to invent, and how to protect communities as well as individuals. Future research should empirically test the recommendations made here, examine enforcement records as AI-specific statutes come into force, and extend the comparison to Francophone and Lusophone jurisdictions, whose civil-law traditions may yield different answers. The companion question, how AI is itself changing the practice of law in Africa, is the subject of a separate study.

Ethical Considerations

This study is a doctrinal and comparative analysis of publicly available legal instruments, judicial decisions, policy documents and published scholarship. It did not involve human participants, personal data, or animals, so ethical approval was not required.

Conflict Of Interest

The authors declare that they have no conflict of interest.

Data Availability

No new data were generated or analysed in this study. All primary and secondary sources relied upon are publicly available and are listed in the References.

REFERENCES

1. Abdulrauf, L. A. (2021). Giving “teeth” to the African Union towards advancing compliance with data privacy norms. Information & Communications Technology Law.
2. AllAfrica. (2025, November 10). Nigeria set to lead Africa in digital economy, e-governance as bill nears presidential assent. https://allafrica.com/stories/202511110110.html
3. Birhane, A. (2020). Algorithmic colonization of Africa. SCRIPTed, 17(2), 389–409. https://doi.org/10.2966/scrip.170220.389
4. Bowmans. (2026, April 23). Kenya: Artificial Intelligence Bill, 2026 – Proposed too soon? https://bowmanslaw.com/insights/kenya-artificial-intelligence-bill-2026-proposed-too-soon/
5. Bradford, A. (2020). The Brussels effect: How the European Union rules the world. Oxford University Press.
6. BusinessDay. (2026). Nigeria set to pass AI law, among first in Africa to regulate sector. https://businessday.ng/technology/article/nigeria-set-to-pass-ai-law-among-first-in-africa-to-regulate-sector/
7. Capital FM. (2026, August 21). Kenya moves to regulate AI, but who will call the shots? https://capitalfm.africa/kenya-moves-to-regulate-ai-but-who-will-call-the-shots/
8. Chambers and Partners. (2025). Fintech 2025: Egypt. https://practiceguides.chambers.com/practice-guides/fintech-2025/egypt
9. Cliffe Dekker Hofmeyr. (2026). Commentary on South Africa’s National Draft Artificial Intelligence Policy. https://www.cliffedekkerhofmeyr.com/en/news/publications/2026/South-Africa/Technology-Communications/corporate-communication-and-technology-communications-alert-commentary-on-south-sfricas-national-draft-artificial-intelligence-policy
10. Digital Policy Alert. (n.d.-a). Nigeria’s AI governance approach. Retrieved October 14, 2026, from https://digitalpolicyalert.org/digest/nigeria-ai-governance-approach
11. Digital Policy Alert. (n.d.-b). National Council for Artificial Intelligence unveiled second edition of National AI Strategy 2025–2030. Retrieved October 14, 2026, from

https://digitalpolicyalert.org/event/41790-national-council-for-artificial-intelligence-unveiled-second-edition-of-national-ai-strategy-2025-2030
12. ENSafrica. (2025, October 30). The guiding principles of AI usage in the legal profession. https://www.ensafrica.com/news/detail/10927/the-guiding-principles-of-ai-usage-in-the-leg
13. European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L series.
14. Gwagwa, A., Kazim, E., & Hilliard, A. (2022). The role of the African value of Ubuntu in global AI inclusion discourse: A normative ethics perspective. Patterns, 3(4), 100462. https://doi.org/10.1016/j.patter.2022.100462
15. K&L Gates. (2026, August 3). EU Digital Omnibus on AI enters into force. Mondaq. https://www.mondaq.com/eu-digital-omnibus-on-ai-enters-into-force/1825722
16. Katiba Institute and Others v Worldcoin Foundation and Others (High Court of Kenya, Judicial Review Division, May 5, 2025).
17. Legal 500. (2026). Egypt: Artificial intelligence. https://www.legal500.com/guides/chapter/egypt-artificial-intelligence/
18. Legrand, P. (1997). The impossibility of "legal transplants". Maastricht Journal of European and Comparative Law, 4(2), 111–124.
19. Makulilo, A. B. (Ed.). (2016). African data privacy laws. Springer.
20. Mavundla v MEC: Department of Co-operative Government and Traditional Affairs KwaZulu-Natal and Others, [2025] ZAKZPHC 2 (High Court of South Africa, KwaZulu-Natal Division, Pietermaritzburg, January 8, 2025).
21. Meta Platforms Inc and WhatsApp LLC v Federal Competition and Consumer Protection Commission (Competition and Consumer Protection Tribunal, Nigeria, April 25, 2025).
22. Mhlambi, S. (2020). From rationality to relationality: Ubuntu as an ethical and human rights framework for artificial intelligence governance (Carr Center Discussion Paper Series). Harvard Kennedy School.
23. Michalsons. (2025). Mavundla v MEC: Department of Co-operative Government and Traditional Affairs KwaZulu-Natal. https://www.michalsons.com/blog/mavundla-v-mec-department-of-co-operative-government-and-traditional-affairs-kwazulu-natal-genai/77431
24. Mobile World Live. (2026). Nigeria to pioneer Africa AI legislation. https://www.mobileworldlive.com/ai-cloud/nigeria-to-pioneer-africa-ai-legislation/
25. Northbound Processing (Pty) Ltd v South African Diamond and Precious Metals Regulator and Others, Case No. 2025-072038 (High Court of South Africa, Gauteng Division, June 30, 2025).
26. OECD. (2024). Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449; adopted 2019, revised 2024). Organisation for Economic Co-operation and Development.
27. People Daily. (2026, January 22). Why Worldcoin erased Kenyans' biometric data. https://peopledaily.digital/insights/why-worldcoin-erased-kenyans-biometric-data
28. Reuters. (2026, May 26). South Africa targets January 2027 for revised AI policy after earlier withdrawal. Engineering News. https://engineeringnews.co.za/print-version/south-africa-targets-january-2027-for-revised-ai-policy-after-earlier-withdrawal-2026-05-26
29. SAnews. (2026, April 26). Minister announces withdrawal of draft AI Policy. South African Government News Agency. https://www.sanews.gov.za/south-africa/minister-announces-withdrawal-draft-ai-policy
30. Smuha, N. A. (2021). From a "race to AI" to a "race to AI regulation": Regulatory competition for artificial intelligence. Law, Innovation and Technology, 13(1), 57–84. https://doi.org/10.1080/17579961.2021.1898300
31. Techpoint Africa. (2026). Nigeria eyes passage of AI law to lead regulation push in Africa. https://techpoint.africa/news/nigeria-to-pass-ai-law/
32. Techweez. (2026, July 7). Kenya's AI policy, as the government sees it. https://techweez.com/2026/07/07/kenyas-ai-policy-as-the-government-sees-it/
33. UNESCO. (2021). Recommendation on the ethics of artificial intelligence. United Nations Educational, Scientific and Cultural Organization.
34. Watson, A. (1974). Legal transplants: An approach to comparative law. Scottish Academic Press.