

Standard Makers, Not Standard Takers: The Case for a Rights-Centred AI Regulatory Framework in Africa's Digital Transformation

Fope Agbede*

Abstract

Africa is at an inflection point. The African Union's endorsement of the Continental AI Strategy at its 45th Executive Council Session in Accra in July 2024 was a bold signal that the continent intends to be an active participant in shaping the future of artificial intelligence, not merely a recipient of technologies and rules designed elsewhere. That ambition is admirable. However, the execution tells a more sobering story.

Across the continent, governments are racing to deploy AI in security operations, economic forecasting, border management, and public service delivery, often ahead of any legal framework capable of governing it. By early 2026, while 44 African countries had enacted data protection laws, the overwhelming majority still lacked dedicated, enforceable AI legislation. Nigeria, one of Africa's largest economies, published its draft National AI Strategy in August 2024 and formally launched it in April 2025, but as of today still has no standalone AI Act, leaving a patchwork of the Nigeria Data Protection Act 2023, the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, and several consolidated bills that are yet to complete their legislative cycle. This pattern repeats itself from Nairobi to Accra to Pretoria.

This paper argues that the gap between Africa's AI ambitions and its legal infrastructure is not merely a technical oversight, it is also a governance crisis with direct consequences for human rights, economic stability, and security. When AI systems are deployed in conflict-prone or economically fragile environments without accountability frameworks, the populations most at risk are those the technology was supposedly meant to serve. Africa does not need to copy the EU AI Act or defer to US frameworks. It needs rights-centred, locally grounded regulation that reflects African realities, protects African citizens, and positions the continent as a rule-maker in global AI governance. Thus, this paper charts what that framework should look like.

Keywords: Artificial Intelligence, Digital Transformation, AI Governance, African Union Continental AI Strategy, Nigeria Data Protection Act 2023, Human Rights, Economic Stability, Security

* Fope Agbede is the Team Lead of Compliance at [Smith and Partners LP](#), Lagos, Nigeria. He can be reached at Fopefoluwa.Agbede@splp-law.com

1. Introduction

Something significant is happening across Africa. From the smallholder farmer in Kano consulting an AI-powered weather prediction tool on a basic mobile phone, to the fintech startup in Nairobi deploying machine learning models for credit scoring, to the Egyptian government unveiling Karnak, its national large language model at the AI Everything MEA Summit in Cairo in February 2026, artificial intelligence is no longer a distant aspiration for the continent. It is here, it is moving fast, and it is reshaping the terms on which millions of Africans live, work, and interact with the state.

The numbers tell a compelling story. The African Development Bank projects that inclusive AI deployment could generate up to one trillion dollars in additional GDP by 2035, nearly one third of the continent's current economic output.¹ McKinsey estimates that generative AI alone, deployed at scale, could unlock between sixty-one billion and one hundred and three billion dollars in annual incremental economic value across African sectors.² The AI market on the continent is projected to grow at a compound annual growth rate of over 27%, reaching an estimated market volume of 16.53 billion dollars by 2030.³ In February 2026, the African Development Bank and the United Nations Development Programme jointly launched the AI 10 Billion Initiative at the Nairobi AI Forum, a continental fund designed to mobilise up to ten billion dollars by 2035 and unlock forty million new jobs across the continent.⁴ These are not theoretical projections. They reflect a continent that has made a deliberate and confident choice to embed AI at the centre of its development agenda.

The political architecture supporting this ambition is also substantial. In July 2024, the African Union Executive Council endorsed the Continental AI Strategy at its 45th Ordinary Session in Accra, Ghana, committing all 55 member states to an Africa-centric, development-focused, and ethically grounded approach to AI.⁵ The Strategy aligns with AU Agenda 2063 and the Sustainable Development Goals, identifies five key focus areas including harnessing AI's benefits and minimising risks, and sets out a

¹ African Development Bank, *Africa's AI Productivity Gain: Pathways to Labour Efficiency, Economic Growth and Inclusive Transformation* (African Development Bank 2025).

² McKinsey & Company, 'Leading, Not Lagging: Africa's Gen AI Opportunity' (McKinsey & Company, May 2025) <https://www.mckinsey.com/capabilities/quantumblack/our-insights/leading-not-lagging-africas-gen-ai-opportunity> accessed 18 July 2026.

³ Statista, 'Artificial Intelligence Market in Africa' (Statista Market Forecast, 2025) <https://www.statista.com/outlook/tmo/artificial-intelligence/africa> accessed 18 July 2026.

⁴ African Development Bank and UNDP, 'African Development Bank, UNDP and Partners Launch the AI 10 Billion Initiative during 2026 Nairobi AI Forum' (African Development Bank, 23 February 2026) <https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-undp-and-partners-launch-ai-10-billion-initiative-during-2026-nairobi-ai-forum-91104> accessed 18 July 2026.

⁵ African Union, *Continental AI Strategy* (African Union, 45th Ordinary Session of the AU Executive Council, Accra, Ghana, 18-19 July 2024).

phased implementation roadmap running from 2025 to 2030.⁶ At the national level, countries including Nigeria, Kenya, Rwanda, Egypt, South Africa, and Mauritius have all developed or are actively developing national AI strategies and governance frameworks.⁷ By early 2026, 44 African countries had enacted data protection laws, and 38 had established functional Data Protection Authorities.⁸

However, despite all this momentum, something is deeply wrong with the picture. Africa is building an AI-powered future on a legal foundation that is, in too many places, either absent, fragmented, or borrowed wholesale from frameworks designed for entirely different contexts. The African Union's Continental AI Strategy is not a binding instrument. Nigeria, the continent's most populous nation and largest economy, published its draft National AI Strategy in August 2024 and formally launched it in April 2025, but still has no standalone AI Act, leaving a patchwork of the Nigeria Data Protection Act 2023, the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, and several consolidated bills yet to complete their legislative cycle.⁹ South Africa, despite its draft National AI Policy Framework published in October 2024, has no comprehensive AI legislation in force.¹⁰ In essence, across the African continent, AI is being deployed in security operations, predictive policing, border surveillance, and economic decision-making in environments where the populations most affected have no legal recourse if those systems get it wrong.

This paper argues that the gap between Africa's AI ambitions and its legal infrastructure is not a footnote. Rather, it is the central challenge of Africa's digital transformation. A continent that deploys AI without enforceable rights-based governance frameworks does not simply risk technological failure. It risks repeating, at speed and at scale, the same patterns of exclusion, exploitation, and ungoverned power that have historically stunted Africa's development. The African Union's own Continental AI Strategy captures it well when it calls on member states to be rule-makers rather than rule-takers in global AI governance.¹¹ This paper takes that call seriously and asks what it will actually take to get there.

⁶ *ibid.*

⁷ Tech In Africa, 'AI Regulation in Africa 2026: New Laws, Compliance Risks, and Startup Opportunities' (Tech In Africa, 25 February 2026) <https://www.techinafrica.com/ai-regulation-africa-2026-new-laws-compliance-startup-opportunities/> accessed 18 July 2026.

⁸ *ibid.*

⁹ IAPP, 'Nigeria Moves Toward Comprehensive AI Regulation' (IAPP, April 2026) <https://iapp.org/news/a/nigeria-moves-toward-comprehensive-ai-regulation> accessed 19 July 2026.

¹⁰ Adams & Adams, 'AI in Africa: Regulations are Catching Up and the Courts are Already There' (Adams & Adams, April 2026) <https://www.adams.africa/danielle-van-deventer/ai-in-africa-regulations-are-catching-up-and-the-courts-are-already-there/> accessed 19 July 2026.

¹¹ African Union (n 5).

2. The African AI Landscape: Promise and the Regulatory Vacuum

Africa's relationship with AI is best understood not as a single story but as a collection of overlapping stories, moving at different speeds, in different directions, and with very different consequences for the people caught in their path. Some of those stories are genuinely exciting. Others are deeply troubling. And the uncomfortable truth is that the legal profession across the continent has not yet decided which story it wants to help tell.

Start with the promise. Africa holds the world's youngest population, the fastest-growing digital economy on the planet, and a continent-wide entrepreneurial energy that no amount of infrastructure deficit has managed to extinguish.¹² The International Finance Corporation projects that the strategic adoption of AI could add up to 234 billion dollars to Africa's GDP by 2030.¹³ The African Development Bank goes further, projecting that inclusive AI deployment could contribute up to one trillion dollars in additional GDP by 2035, nearly one third of the continent's current economic output.¹⁴ Generative AI alone, McKinsey estimates, could unlock between sixty-one billion and one hundred and three billion dollars in annual incremental economic value across African sectors.¹⁵ These projections are not wishful thinking. They are grounded in real and visible momentum. In Kenya, smallholder farmers are already using AI-powered models to predict rainfall patterns and optimise crop cultivation. In Nigeria, personalised education platforms are using machine learning to offer targeted learning. In South Africa, healthcare providers are integrating large language models into clinical workflows.¹⁶

The political response to this momentum has been ambitious. The African Union's endorsement of the Continental AI Strategy in July 2024 was a genuine milestone, committing all 55 member states to an Africa-centric approach that prioritises ethics, inclusivity, and digital sovereignty.¹⁷ At the national level, countries including Nigeria, Kenya, Rwanda, Egypt, South Africa, and Mauritius have developed or are actively developing national AI strategies.¹⁸ Nigeria jumped 31 places in the Government AI Readiness Index in 2025, now ranking 72nd out of 195 countries.¹⁹ By early 2026, 44 African countries had

¹² Mastercard, *AI in Africa 2025: Harnessing the Transformative Power* (Mastercard, August 2025).

¹³ Federal Ministry of Communications, Innovation and Digital Economy (Nigeria), 'National Artificial Intelligence Strategy' (FMCIDE, 2024) <https://fmcide.gov.ng/initiative/nais/> accessed 20 July 2026.

¹⁴ African Development Bank, *Africa's AI Productivity Gain: Pathways to Labour Efficiency, Economic Growth and Inclusive Transformation* (African Development Bank 2025) (n 1).

¹⁵ McKinsey & Company (n 2).

¹⁶ Mastercard (n 12).

¹⁷ African Union, *Continental AI Strategy* (n 5).

¹⁸ Tech In Africa (n 7).

¹⁹ *ibid.*

enacted data protection laws, and 38 had established functional Data Protection Authorities.²⁰ Thus, it can't be denied that the architecture of ambition is real and it deserves to be acknowledged.

But architecture of ambition is not the same thing as architecture of governance. And it is on the governance side that the picture becomes far more sobering.

The Continental AI Strategy, for all its vision, is not a binding legal instrument. It cannot be enforced. It creates no liability. It establishes no individual rights. It is, at its core, a political declaration dressed in the language of a regulatory framework. This matters enormously because in the absence of binding rules, what fills the vacuum is not careful deliberation. What fills the vacuum is speed, money, and power. In 2025, 83% of AI funding across the continent was concentrated in just four nations, namely Kenya, Nigeria, South Africa, and Egypt, creating what one analyst has aptly described as a development-governance paradox where rules exist on paper but cannot be enforced without local compute capacity.²¹ Africa currently holds less than 1% of global data centre capacity, meaning that the infrastructure powering Africa's AI ambitions remains largely in the hands of foreign providers.²² AWS, Microsoft Azure, and Google Cloud dominate the global cloud market, and all three are expanding aggressively across the continent.²³

The consequence of this regulatory vacuum is not abstract. It is playing out in real time, in ways that should alarm every African lawyer and policymaker. At least 11 African governments have spent over two billion dollars on Chinese-built AI-powered surveillance infrastructure, including facial recognition systems, biometric data collection tools, and smart city cameras deployed across public spaces.²⁴ Nigeria tops the list, having spent 470 million dollars on 10,000 smart cameras alone.²⁵ These systems were marketed as tools for crime prevention and urban management. In practice, research by the African Digital Rights Network and the Institute of Development Studies found that they are being used to monitor activists, track protesters, and silence dissent, with a chilling effect on freedoms of assembly

²⁰ *ibid.*

²¹ Atomic Mail, 'AI Regulation News: 2025 Global Changes, 2026 Watchlist' (Atomic Mail) <https://atomicmail.io/blog/ai-regulation-news-global-changes-and-watchlist> accessed 21 July 2026.

²² CircleID, 'Africa's AI Governance Crisis Is Not a Regulatory Gap, It Is a Sovereignty Emergency' (CircleID, April 2026) <https://circleid.com/posts/africas-ai-governance-crisis-is-not-a-regulatory-gap-it-is-a-sovereignty-emergency> accessed 21 July 2026.

²³ *ibid.*

²⁴ CIVICUS, 'AI: African Governments Are Using "Smart City" Systems to Monitor Dissent and Consolidate State Control' (CIVICUS Lens, April 2026) <https://lens.civicus.org/interview/ai-african-governments-are-using-smart-city-systems-to-monitor-dissent-and-consolidate-state-control/> accessed 21 July 2026.

²⁵ iAfrica, 'AI Surveillance Spending Tops \$2 Billion Across 11 African Nations, Raising Rights Concerns' (iAfrica, March 2026) <https://iafrica.com/ai-surveillance-spending-tops-2-billion-across-11-african-nations-raising-rights-concerns/> accessed 22 July 2026.

and expression.²⁶ In Uganda and Zimbabwe, AI-powered facial recognition has been used specifically to suppress political opposition.²⁷ In Kenya, surveillance systems were deployed against Gen Z protesters.²⁸ Across Algeria, surveillance tools introduced as part of smart city projects have in practice become primarily instruments of security forces rather than tools of genuine public safety.²⁹

This is the regulatory vacuum made visible. When AI is deployed at scale, with public funds, against the very citizens those systems are supposed to protect, and there is no law that clearly prohibits it, no court that has jurisdiction to stop it, and no regulator empowered to demand accountability, the promise of AI-driven development collapses into something far more dangerous. A 2025 UN expert group report put it plainly: AI systems used for mass surveillance, real-time facial recognition, and predictive policing are incompatible with international human rights law, and states have an obligation to prohibit them.³⁰ Most African states have not done so.

It is worth being direct about what this means. The gap between Africa's AI ambitions and its legal infrastructure is not simply a technical oversight waiting to be corrected. It reflects a deeper and more troubling pattern. The continent that produced the African Charter on Human and Peoples' Rights in 1981 and adopted the Malabo Convention on Cyber Security and Personal Data Protection in 2014, a convention that only came into force in June 2023, is the same continent where governments are spending hundreds of millions of dollars deploying AI surveillance systems without legal authorisation, public debate, or any meaningful mechanism for redress. Something has gone badly wrong with the sequencing of priorities, and the legal profession has both the standing and the responsibility to say so.

²⁶ CIVICUS (n 24).

²⁷ *ibid.*

²⁸ *ibid.*

²⁹ *ibid.*

³⁰ JURIST, 'UN Says Use of Artificial Intelligence Must Comply with International Human Rights' (JURIST, June 2025) <https://www.jurist.org/news/2025/06/un-says-use-of-artificial-intelligence-must-comply-with-international-human-rights/> accessed 22 July 2026.

3. AI, Security and the Risk of Ungoverned Technology

There is a seductive logic to the argument that Africa needs AI for security. The continent faces genuine and complex security challenges: jihadist insurgencies in the Sahel, maritime piracy along the Gulf of Guinea, cross-border cybercrime, electoral violence, and the persistent threat of state fragility in conflict-prone regions. AI, on this view, offers tools that cash-strapped and overstretched security agencies desperately need: predictive analytics to anticipate threats, facial recognition to identify suspects, drone surveillance to monitor porous borders, and machine learning models to detect financial crime. The argument is not wrong. The problem is that it is dangerously incomplete. Ungoverned AI in the security space does not simply carry risk. It actively multiplies the very instabilities it is deployed to contain.

The World Economic Forum's Global Cybersecurity Outlook 2026 found that 87% of respondents identified AI-related vulnerabilities as the fastest-growing cyber risk in 2025, and that AI is anticipated to be the most significant driver of change in cybersecurity in the year ahead according to 94% of survey respondents.³¹ This is a global finding, but it lands with particular force on a continent where the infrastructure used to deploy AI systems is largely externally owned, enforcement capacity is still being built, and legal frameworks capable of assigning liability for AI-driven security failures are almost entirely absent. When an AI system used in a European security context fails, there are courts, regulators, and legal remedies available. When an equivalent system fails in an African security context, the question of who bears responsibility is, in most jurisdictions, genuinely unanswerable.

This is not a hypothetical concern. Between December 2025 and January 2026, INTERPOL's Operation Red Card 2.0, involving 16 African countries, resulted in 651 arrests, the seizure of over 4.3 million dollars, the takedown of 1,442 malicious IP addresses, domains, and servers, and the identification of fraud schemes causing estimated losses of around 45 million dollars with 1,247 victims.³² In March 2026, two suspects in Ghana were arrested specifically for creating AI-generated deepfakes impersonating the President and First Lady to facilitate financial scams.³³ These are not the actions of sophisticated state actors, they are the actions of relatively low-skilled criminals exploiting the same regulatory vacuum that governments are failing to close. Deepfake-as-a-service platforms became

³¹ World Economic Forum, *Global Cybersecurity Outlook 2026* (WEF, January 2026) reported in Industrial Cyber, 'WEF Global Cybersecurity Outlook 2026 Flags AI Acceleration, Geopolitical Fractures' (Industrial Cyber, 13 January 2026) <https://industrialcyber.co/reports/wef-global-cybersecurity-outlook-2026-flags-ai-acceleration-geopolitical-fractures-calls-for-shared-responsibility/> accessed 22 July 2026.

³² CircleID (n 22).

³³ *ibid.*

widely available in 2025, making video cloning, voice cloning, and persona simulation accessible to cybercriminals of all skill levels.³⁴ AI-enhanced cyber-attacks surged 180% in 2025 globally, and Africa, with its weaker enforcement architecture, absorbed a disproportionate share of the damage.³⁵

The security threat posed by ungoverned AI on the continent goes beyond cybercrime. It reaches directly into the integrity of democratic governance. Africa's 2023 and 2024 electoral cycles were the first in which AI-generated content featured at scale in political campaigning and disinformation. The 2023 Nigerian presidential election was, by most accounts, the first African election to experience a significant deluge of AI-generated electoral content, including fake celebrity endorsements and, most troublingly, AI-generated audio clips shared hours before polling purportedly revealing candidates' plans to rig the vote.³⁶ Research shows that 60% of disinformation campaigns targeting Africa are foreign-sponsored, primarily from Russia, China, and Gulf states, with West Africa bearing the brunt of these attacks.³⁷ The Africa Center for Strategic Studies documented that AI-generated avatars were used in political influenced campaigns in Burkina Faso.³⁸ A Kremlin-aligned disinformation network, uncovered during Moldova's 2025 parliamentary elections, was found to have paid engagement farms on the continent to amplify pro-Russian narratives through verified African social media accounts.³⁹

The Regional Centre on Small Arms and Light Weapons issued a report, warning that AI-driven technologies including 3D printing and drone manufacturing are accelerating the spread of illicit weapons in East Africa, complicating enforcement and significantly increasing the cost of maintaining security in an already fragile region.⁴⁰ The AU Peace and Security Council convened a dedicated ministerial session on AI and its impact on peace, security, and governance in March 2025 and has since established a high-level Advisory Group with a mandate to report every six months.⁴¹ These

³⁴ Cyble, 'Deepfake-as-a-Service Exploded in 2025: 2026 Threats Ahead' (Cyble, March 2026) <https://cyble.com/knowledge-hub/deepfake-as-a-service-exploded-in-2025/> accessed 24 July 2026.

³⁵ CircleID (n 22).

³⁶ Democracy in Africa, 'AI-Generated Propaganda Threatens African Democracy' (Democracy in Africa, September 2025) <https://democracyinafrica.org/ai-generated-propaganda-threatens-african-democracy/> accessed 24 July 2026.

³⁷ *ibid.*

³⁸ Brookings Institution, 'Building Regional Capacity for AI Safety and Security in Africa' (Brookings, May 2025) <https://www.brookings.edu/articles/building-regional-capacity-for-ai-safety-and-security-in-africa/> accessed 24 July 2026.

³⁹ Centre for Emerging Technology and Security, 'From Deepfake Scams to Poisoned Chatbots: AI and Election Security in 2025' (CETaS, 2025) <https://cetas.turing.ac.uk/publications/deepfake-scams-poisoned-chatbots> accessed 25 July 2026.

⁴⁰ Capital Business, 'AI Weapons Raise Security, Economic Risks in East Africa' (Capital Business, March 2026) <https://www.capitalfm.co.ke/business/2026/03/ai-weapons-raise-security-economic-risks-in-east-africa/> accessed 25 July 2026.

⁴¹ Amani Africa, 'Artificial Intelligence and its Impact on Peace, Security and Governance' (Amani Africa, 19 March 2025) <https://amaniafrica-et.org/artificial-intelligence-and-its-impact-on-peace-security-and-governance/> accessed 26 July 2026.

developments are welcome but belated. The threats were already materialising long before the advisory architecture was assembled.

Perhaps the most revealing dimension of the security problem is the one that connects back to the governance gap examined in the previous section. Across the continent, AI is being deployed by governments themselves in ways that create security threats, rather than them. The deployment of 10,000 AI-powered smart cameras in Nigeria at a cost of 470 million dollars, the installation of AI facial recognition systems in Uganda used against political opponents, and the use of surveillance infrastructure against Gen Z protesters in Kenya are not just human rights issues.⁴² They are also security issues, because governments that use AI to suppress legitimate dissent do not produce stable societies. They produce societies where grievances accumulate without an outlet, where trust in institutions collapses, and where the conditions for serious conflict become entrenched. The International AI Safety Report 2025, which was informed by representatives from Rwanda, Nigeria, and Kenya, warned explicitly that the impacts of highly capable AI on the continent could amount to large-scale setbacks including unparalleled manipulation and more damaging armed conflicts.⁴³

The legal profession's contribution to this conversation must be more than descriptive. It is not enough to catalogue the risks and call for better behaviour. The argument this paper makes is that the security risks of ungoverned AI in Africa are, at their core, a legal infrastructure problem. A system that carries no liability for harmful outcomes will be deployed carelessly. A technology that operates in a jurisdiction with no enforceable accountability framework will be misused by both state and non-state actors. And a continent that allows foreign entities to deploy AI-driven security infrastructure without binding legal constraints on how that infrastructure is used is not enhancing its security. It is outsourcing its sovereignty. The AU Convention on Cyber Security and Personal Data Protection, the Malabo Convention, which only came into force in June 2023, provides a partial foundation. But a convention that took nine years to enter into force and still lacks robust enforcement mechanisms at the national level is, in practice, closer to an aspiration than a legal shield. Africa needs to move faster, and it needs to move deliberately.

⁴² CIVICUS (n 24); iAfrica (n 25).

⁴³ Brookings Institution (n 38).

4. Nigeria as a Case Study: From NDPR to the Digital Sovereignty Bill

Nigeria is worth examining in detail not because it is the worst example of AI governance on the continent, but because it is arguably the most instructive one. As Africa's most populous nation and currently the third largest economy, with a fast-growing technology ecosystem and a demonstrated appetite for legal reform, Nigeria represents what is possible when political will and institutional capacity begin to align around digital governance. It also represents, with uncomfortable clarity, how much further that alignment still needs to go before it can be called adequate for the AI era the continent has already entered.

The story begins with the Nigeria Data Protection Regulation 2019, which was Nigeria's first serious attempt to regulate the processing of personal data. Well-intentioned as it was, the NDPR was fundamentally limited. It lacked statutory legitimacy, derived its force from an administrative agency rather than an Act of the National Assembly, and was enforced by the National Information Technology Development Agency, which did not possess the institutional muscle or legal foundation to compel adherence, particularly from foreign-owned technology companies operating at scale.⁴⁴ The NDPR functioned more as a policy placeholder than a comprehensive legal instrument, and its shortcomings became increasingly difficult to defend as AI-driven data processing accelerated across the economy.

The enactment of the Nigeria Data Protection Act 2023 was a genuine and significant departure. Receiving presidential assent on 12 June 2023, the NDPA elevated data protection from administrative regulation to statutory law, establishing the Nigeria Data Protection Commission as an independent regulatory body with clear statutory powers to issue binding decisions, investigate infractions, sanction non-compliance, and develop guidance frameworks for both private and public actors.⁴⁵ Critically for the AI conversation, Section 37 of the NDPA addresses automated decision-making, providing data subjects with rights in respect of decisions made solely by automated processes that produce legal or similarly significant effects.⁴⁶ This is important because it means that AI systems deployed for credit scoring, loan approvals, insurance underwriting, and other consequential decisions are, at least in principle, subject to a legal framework that demands transparency and human oversight.

⁴⁴ ThisDay Live, 'Ethical Problems in AI and Digital Legislation in Nigeria (Part 2)' (ThisDay, July 2025) <https://www.thisdaylive.com/2025/07/22/ethical-problems-in-ai-and-digital-legislation-in-nigeria-part-2/> accessed 26 July 2026.

⁴⁵ *ibid* s 1; DLA Piper, 'Data Protection Laws in Nigeria' (DLA Piper Data Protection Laws of the World) <https://www.dlapiperdataprotection.com/index.html?t=law&c=NG> accessed 26 July 2026.

⁴⁶ Nigeria Data Protection Act 2023, s 37.

The NDPA's enforcement record already demonstrates that this is not merely a paper regime. The Nigeria Data Protection Commission imposed a fine of 766,242,500 Naira on Multichoice Nigeria in July 2025 following an investigation that found the company had engaged in data processing practices described by the Commission as patently intrusive, unfair, unnecessary, and disproportionate, in violation of Section 37 of the 1999 Constitution of the Federal Republic of Nigeria⁴⁷ which guarantees the right to privacy.⁴⁸ The NDPC separately fined Meta Platforms 32.8 million dollars for violations of data privacy laws, one of the largest penalties yet imposed by the Commission against a foreign technology company which was later challenged in court and an out-of-court settlement adopted as consent judgement.⁴⁹ In August 2025, the NDPC launched investigations into 1,368 organisations across banking, insurance, pension, and gaming sectors.⁵⁰ These are not the actions of a regulator that lacks appetite for enforcement. They are the actions of an institution that is finding its feet and beginning to use them.

In March 2025, the NDPC published the General Application and Implementation Directive, which took effect in September 2025.⁵¹ The GAID provides granular operational rules for Data Controllers of Major Importance, including those deploying large-scale AI models, and clarifies how the NDPA applies to modern data processing techniques such as machine learning and neural networks.⁵² It also introduces the Standard Notice to Address Grievance mechanism, which empowers citizens to demand direct remedial action from AI deployers before escalating to the Commission.⁵³ This is a meaningful innovation as it creates a first-instance accountability layer that does not require a citizen to navigate the full weight of regulatory machinery simply to obtain redress from an AI system that got a consequential decision wrong.

⁴⁷ Constitution of the Federal Republic of Nigeria 1999 (as amended), s 37.

⁴⁸ Nairametrics, 'NDPC Fines Multichoice Nigeria N766.2 Million for Violating NDP Act' (Nairametrics, 6 July 2025) <https://nairametrics.com/2025/07/06/ndpc-fines-multichoice-nigeria-n766-2-million-for-violating-ndp-act/> accessed 26 July 2026.

⁴⁹ The ICIR, 'NDPC Fines Multichoice Nigeria N766 Million Over Data Privacy Violations' (The ICIR, 6 July 2025) <https://www.icirnigeria.org/ndpc-fines-multichoice-nigeria-%E2%82%A6766-million-over-data-privacy-violations/> accessed 26 July 2026, reporting the NDPC's separate \$32.8 million fine against Meta Platforms.

⁵⁰ Premium Times, 'NDPC Issues Compliance Notices to Banks, Insurers, Pension and Gaming Firms' (Premium Times, 26 August 2025) <https://www.premiumtimesng.com/business/816603-ndpc-issues-compliance-notices-to-banks-insurers-pension-and-gaming-firms.html> accessed 26 July 2026.

⁵¹ IAPP, 'From Principles to Practice: Operationalizing Nigeria's Data Protection Act through the GAID' (IAPP, February 2026) <https://iapp.org/news/a/from-principles-to-practice-operationalizing-nigerias-data-protection-act-through-the-gaid> accessed 27 July 2026.

⁵² Regulations.ai, 'Nigeria AI Regulation Overview' (Regulations.ai, January 2026) <https://regulations.ai/regulations/nigeria-summary> accessed 27 July 2026.

⁵³ *ibid.*

However, for all of this genuine progress, Nigeria's AI governance framework remains fundamentally incomplete. Nigeria still has no standalone AI Act. Multiple AI-specific bills have been introduced to the National Assembly since 2021, including the Artificial Intelligence and Robotics Research Regulatory Agency Bill 2021, the National AI and Robotics Sciences Bill 2023, the Control of Usage of Artificial Intelligence Technology Bill 2023, and the National Artificial Intelligence Regulatory Authority Bill 2024, and as of December 2024 these had been consolidated for second reading without completing their legislative cycle.⁵⁴ In 2025, the National Artificial Intelligence Commission (Establishment) Bill was introduced, proposing a dedicated National AI Commission to oversee AI development across all sectors.⁵⁵ The Digital Sovereignty, AI Governance, and Fair Compensation Bill was presented in February 2025, targeting the extraction and monetization of Nigerian data by foreign digital companies and seeking to require that data generated within Nigeria remain within Nigeria.⁵⁶ As of the time of writing, neither bill has been enacted.

This legislative lag matters enormously. Nigeria's National AI Strategy, published in August 2024 and formally launched in April 2025, is built around five pillars of infrastructure, talent, adoption, ethics, and governance, and sets out a roadmap that is genuinely ambitious.⁵⁷ But a strategy document, however well-crafted, is not law. It creates no enforceable obligations. It establishes no liability for harm. It gives no citizen a right of action when an AI system deployed against them causes loss or injury. The NDPA provides a partial foundation, but it was designed for data protection, not for the full range of AI-specific risks that the country faces. The gap between what the NDPA can address and what a comprehensive AI Act would need to cover is the space in which ungoverned AI currently operates in Nigeria, and that space is large.

There is also the question of what Nigeria's AI governance journey teaches the rest of the continent. Nigeria's experience demonstrates two things with particular clarity. First, that data protection law, while necessary, is not sufficient as the primary vehicle for AI regulation. The NDPA's Section 37 protections for automated decision-making are valuable, but they address only a narrow slice of the AI risk landscape. They say nothing enforceable about AI-powered surveillance, algorithmic bias in public service delivery, the use of AI in military or security operations, or the liability of foreign companies

⁵⁴ IAPP, 'Nigeria Moves Toward Comprehensive AI Regulation' (n 9).

⁵⁵ *ibid.*

⁵⁶ TechHive Advisory Africa, 'Nigeria: A 2025 Retrospective and 2026 Outlook' (TechHive Advisory Africa, December 2025) <https://www.techhiveadvisory.africa/insights/nigeria-a-2025-retrospective-and-2026-outlook> accessed 27 July 2026.

⁵⁷ Nairametrics, 'Nigeria Launches National AI Strategy to Drive AI Development and Productivity' (Nairametrics, 16 April 2025) <https://nairametrics.com/2025/04/16/nigeria-launches-national-ai-strategy-to-drive-ai-development-and-productivity/> accessed 27 July 2026.

whose AI systems cause harm in Nigeria. Second, Nigeria's experience demonstrates that institutional capacity, once built, can move faster than many expect. The NDPC's enforcement record over 2024 and 2025 is proof that an independent, well-resourced regulatory body with clear statutory powers can impose meaningful accountability on even the most powerful digital companies operating on the continent. The lesson for the rest of Africa is that the institutional architecture matters as much as the legal text itself, and that both need to be built simultaneously, not sequentially.

5. What a Rights-Centred Framework Should Look Like

The question is not whether Africa needs an AI regulatory framework. That debate, to the extent it was ever genuinely open, has been settled by events. The question is what kind of framework Africa needs, who should shape it, and how it should be built in a way that reflects African realities rather than simply transplanting regulatory models designed for entirely different political, economic, and institutional contexts. This section sets out what this paper believes a rights-centred AI regulatory framework for Africa should look like, drawing on the evidence examined in the preceding sections and on the lessons, both instructive and cautionary, that can be derived from existing global approaches.

5.1 Start With Binding Law, Not Strategy Documents

The most fundamental point is also the most obvious one, and it bears stating directly because African governments continue to resist it. Strategy documents, however ambitious, do not create enforceable rights. They do not give citizens a cause of action. They do not impose liability on technology companies. They do not empower regulators to issue binding decisions or impose sanctions. Africa needs binding AI legislation, enacted through democratic legislative processes, not policy papers published by ministries and left to gather dust while the technology they purport to govern accelerates past them.

The European Union's approach is instructive here, though not as a model to be copied wholesale. The EU Artificial Intelligence Act, which entered into force on 1 August 2024 and has been progressively applying its provisions since February 2025, establishes a risk-based classification system that categorises AI systems according to the level of risk they pose and imposes increasingly stringent obligations on higher-risk systems.⁵⁸ Prohibited practices under the Act, including real-time remote biometric identification systems in public spaces, untargeted scraping of the internet or CCTV material to create facial recognition databases, and social scoring systems, became effective in February 2025.⁵⁹ The significance of this for Africa is not that African countries should adopt the EU AI Act. It is that when the EU decided it had a problem with ungoverned AI, it passed a law. Africa's response to the same problem has been to publish a strategy. That asymmetry is untenable.

⁵⁸ 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) OJ L, 2024/1689, 12.7.2024 (EU AI Act).

⁵⁹ EU AI Act (n 59) art 5; European Parliament, 'EU AI Act: First Regulation on Artificial Intelligence' (European Parliament, February 2025) <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> accessed 27 July 2026.

What Africa needs is binding national AI legislation that, at a minimum, establishes clear prohibited uses of AI, creates a risk-based classification system tailored to African contexts, mandates human rights impact assessments before high-risk AI systems are deployed, confers enforceable rights on individuals affected by AI decisions, and establishes independent regulatory bodies with genuine investigative and sanctioning powers. The AU High Level Policy Dialogue on AI, convened in Addis Ababa in May 2025, called explicitly for the establishment of a Continental AI Governance Mechanism founded in ethical principles, democratic values, and cooperation.⁶⁰ That call needs to be translated into treaty language and ratified by member states, not left as a communiqué.

5.2 Mandate Human Rights Impact Assessments

One of the most practical and immediately implementable elements of a rights-centred framework is the mandatory Human Rights Impact Assessment for high-risk AI deployments. The 2025 State of Internet Freedom in Africa report, drawing on research across 14 African countries, recommended instituting mandatory human rights impact assessments as a core element of AI governance reform.⁶¹ The African Commission on Human and Peoples' Rights' own draft study on AI and emerging technologies, published in March 2025, grounded this recommendation directly in the African Charter on Human and Peoples' Rights, noting that the Charter's provisions on equality and non-discrimination require that AI systems be designed and implemented in ways that do not perpetuate or exacerbate existing biases.⁶² Article 17 of the International Covenant on Civil and Political Rights, to which most African states are party, protects the right to privacy, and successive reports of the UN Special Rapporteur on the right to privacy have explicitly cautioned against mass surveillance, data exploitation, and unregulated AI use in public decision-making.⁶³

A mandatory Human Rights Impact Assessment requirement would mean that before any government agency deploys an AI system in policing, border management, social welfare distribution, or any other domain with significant consequences for individuals, it must first conduct and publish a structured

⁶⁰ African Union, 'Communiqué of the High Level Policy Dialogue on the Development and Regulation of AI in Africa' (African Union, 17 May 2025) <https://au.int/en/pressreleases/20250517/communique-high-level-policy-dialogue-ai-africa> accessed 28 July 2026.

⁶¹ CIPESA, 'State of Internet Freedom in Africa Report: Navigating the Implications of AI on Digital Democracy in Africa' (CIPESA, September 2025) <https://cipesa.org/2025/09/state-of-internet-freedom-in-africa-report/> accessed 28 July 2026.

⁶² African Commission on Human and Peoples' Rights, *Draft Study on Artificial Intelligence, Robotics and Emerging Technologies in Africa* (ACHPR, March 2025); African Charter on Human and Peoples' Rights arts 2, 3.

⁶³ International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17; AfricLaw, 'International Privacy Day 2026: Why Privacy Is Africa's Democratic Imperative in the Age of Data, AI, and Surveillance' (AfricLaw, 28 January 2026) <https://africlaw.com/2026/01/28/international-privacy-day-2026-why-privacy-is-africas-democratic-imperative-in-the-age-of-data-ai-and-surveillance/> accessed 28 July 2026.

assessment of the potential human rights impacts of that system. This is not a bureaucratic exercise. It is a mechanism for surfacing, before deployment, the kinds of harms that are currently only becoming visible after they have already been inflicted on communities with the least power to seek redress.

5.3 Build Independent Regulatory Institutions With Real Teeth

Nigeria's experience with the NDPC demonstrates that institutional design matters as much as legislative text. An independent regulatory body with clear statutory powers, adequate resources, and genuine political insulation from the entities it regulates can impose meaningful accountability even on the most powerful technology companies operating on the continent. The NDPC's 32.8 million dollar fine against Meta Platforms which later led to a consent judgment, and its 766 million naira fine against Multichoice Nigeria were not achieved through goodwill. They were achieved through statutory authority grounded in the Nigeria Data Protection Act 2023.⁶⁴

African AI regulators need equivalent foundations. They need statutory independence, not ministerial discretion. They need financial resources that do not depend on the political goodwill of the governments they are sometimes required to hold accountable. They need technical expertise, which means investment in training and in attracting specialists who understand both the technology and its legal implications. And they need the power to act on their findings, not merely to report them. Kenya's Office of the Data Protection Commissioner issued compliance notices to over 1,300 organisations in 2025 and imposed fines on digital lenders for unlawful data processing.⁶⁵ South Africa's Artificial Intelligence Institute of South Africa, launched in partnership with the University of Johannesburg and Tshwane University of Technology, is tasked with setting technical standards and guiding public sector AI initiatives.⁶⁶ These are the kinds of institutional investments that need to be replicated and strengthened across the continent, with dedicated AI mandates rather than data protection mandates stretched to cover AI by implication.

5.4 Prohibit Ungoverned AI Surveillance Explicitly

It is not enough for African AI frameworks to regulate surveillance. They must prohibit its most harmful forms outright. The evidence examined in this paper is unambiguous: AI-powered mass surveillance deployed without legal authorisation, independent oversight, and public accountability is being used across the continent not to enhance security but to suppress dissent, monitor political opponents, and

⁶⁴ Nairametrics (n 48).

⁶⁵ Tech In Africa (n 7).

⁶⁶ *ibid.*

chill the exercise of constitutionally protected rights. At least eleven African governments have collectively spent over two billion dollars on Chinese-built surveillance infrastructure deployed with little regulation and no independent evidence of its effectiveness.⁶⁷ Across Uganda, Zimbabwe, Kenya, Algeria, and Mozambique, these systems are functioning as instruments of political control rather than genuine public safety tools.⁶⁸

A rights-centred framework must therefore include explicit prohibitions on real-time facial recognition in public spaces without prior judicial authorisation, AI-powered mass surveillance deployed without a specific legal basis and proportionality assessment, and the use of predictive policing systems that have not been independently audited for bias and accuracy. These prohibitions need to be backed by criminal liability for officials who deploy prohibited systems, and by civil remedies for individuals whose rights have been violated. The African Charter on Human and Peoples' Rights already provides the normative foundation for these prohibitions.⁶⁹ What is missing is their translation into enforceable domestic law.

5.5 Africa Must Shape Global AI Standards, Not Simply Receive Them

The final and perhaps most politically important element of a rights-centred framework is the one that connects back to the core thesis of this paper. Africa's AI governance challenge is not only domestic. It is geopolitical. The continent is currently caught between competing external AI governance models: the EU's rights-based and heavily regulated approach on one hand, and the US and Chinese approaches on the other, which are driven more by strategic and commercial considerations than by the protection of individual rights. DeepSeek's adoption across Africa is surging, largely driven by its accessibility and by partnerships with companies such as Huawei.⁷⁰ The cloud infrastructure powering Africa's AI ambitions is overwhelmingly controlled by AWS, Microsoft Azure, and Google Cloud.⁷¹ All these, while Africa only currently holds less than 1% of global data centre capacity.⁷²

This dependency is not merely an infrastructure problem but a sovereignty problem. A continent that allows its AI regulatory agenda to be shaped by the priorities of foreign technology companies and foreign governments is not governing itself, It is being governed. The AU's own Continental AI Strategy

⁶⁷ CIVICUS (n 24).

⁶⁸ *ibid.*

⁶⁹ African Charter on Human and Peoples' Rights, arts 2, 3, 9, 12.

⁷⁰ Microsoft AI Economy Institute, 'Global AI Adoption 2025' (Microsoft, January 2026) <https://www.microsoft.com/en-us/corporate-responsibility/topics/ai-economy-institute/reports/global-ai-adoption-2025/> accessed 29 July 2026.

⁷¹ CircleID (n 22).

⁷² *ibid.*

warned against this, calling on member states to be standard makers rather than standard takers.⁷³ African countries need to participate actively and assertively in global AI governance forums, including the UN process on AI governance, the OECD AI principles framework, and the emerging Council of Europe Framework Convention on Artificial Intelligence, the first legally binding international AI treaty, which was signed by the EU on behalf of its member states in September 2024.⁷⁴ Africa does not need to sign agreements written for other contexts. It needs to be in the room where those agreements are written, with a clear and unified position that reflects African values, African development priorities, and the rights of African citizens.

⁷³ African Union, *Continental AI Strategy* (n 5).

⁷⁴ Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (opened for signature 5 September 2024, CETS No 225); EU AI Act recital 5.

6. Conclusion

There is a phrase that appeared in the coverage of the inaugural Global AI Summit on Africa, held in Kigali in April 2025, that deserves to be taken seriously as both an aspiration and a warning. African policymakers, gathered to declare AI a strategic continental priority and to commit to collaboratively building the digital infrastructure, datasets, compute capabilities, and governance frameworks the continent needs, spoke of the importance of moving from strategy to implementation, from vision to innovation, and from dialogue to impact.⁷⁵ Those are the right words. The question is whether Africa's legal and policy communities will provide the architecture that makes that movement possible, or whether the continent will continue to build ambitious visions on foundations that cannot support them.

This paper has argued, through the evidence of the preceding sections, that the central challenge of Africa's AI transformation is not technological. It is legal. Africa has the ambition. It has the demographic dividend, with one in four people in the world projected to live in Africa by 2050.⁷⁶ It has growing institutional momentum, demonstrated by the AU Continental AI Strategy, the Nairobi AI Forum, the AI 10 Billion Initiative, and the High Level Policy Dialogue in Addis Ababa. What it does not yet have, in most jurisdictions and certainly at the continental level, is the binding legal infrastructure that would make all of that momentum accountable, enforceable, and genuinely rights-protective.

The consequences of that gap are not hypothetical. They are playing out right now, on the streets of Kampala where facial recognition tracks political opponents, in the server rooms of foreign cloud providers that control the infrastructure African AI runs on, in the feed of every African social media user being served AI-generated disinformation designed by foreign actors to destabilise their democracies, and in the decisions of credit scoring algorithms trained on biased datasets that systematically deny loans to women-led businesses despite their demonstrably better repayment

⁷⁵ African Union, 'Africa Declares AI a Strategic Priority as High-Level Dialogue Calls for Investment, Inclusion, and Innovation' (African Union, 17 May 2025) <https://au.int/en/pressreleases/20250517/africa-declares-ai-strategic-priority-investment-inclusion-and-innovation> accessed 29 July 2026; Carnegie Endowment for International Peace, 'What's Next for Africa's AI Future?' (Carnegie, December 2025) <https://carnegieendowment.org/carnegie-africa-program-newsletter/whats-next-for-africas-ai-future> accessed 29 July 2026.

⁷⁶ Carnegie Endowment for International Peace, 'Understanding Africa's AI Governance Landscape: Insights From Policy Practice and Dialogue' (Carnegie, September 2025) <https://carnegieendowment.org/posts/2025/09/understanding-africas-ai-governance-landscape-insights-from-policy-practice-and-dialogue> accessed 29 July 2026.

records.⁷⁷ These are not edge cases. They are the predictable and documented consequences of deploying powerful technology in an environment where the law has not kept pace.

This paper has proposed a framework built around five interconnected pillars: binding legislation rather than strategy documents; mandatory human rights impact assessments before high-risk AI systems are deployed; independent regulatory institutions with genuine statutory authority and technical capacity; explicit prohibitions on ungoverned AI surveillance; and active African participation in the shaping of global AI standards rather than passive acceptance of frameworks designed elsewhere. None of these proposals is radical. All of them are grounded in existing African legal norms in the African Charter on Human and Peoples' Rights, the Malabo Convention, the ICCPR, and in the AU's own Continental AI Strategy. The gap is not between African values and what good AI governance requires, it is between those values and what African law currently enforces.

The legal profession has a particular and irreplaceable role to play in closing that gap. Lawyers across the continent are uniquely positioned to translate the technical and ethical dimensions of AI governance into language that legislatures can enact, courts can apply, and citizens can invoke. The Africa AI Policy Fellowship, launched by Lawyers Hub in 2026, reflects a growing recognition that this translation work requires deliberate investment in a generation of legal professionals who understand both the technology and its governance implications.⁷⁸ African Bar Associations, including the African Bar Association whose conference this paper addresses, have both the standing and the responsibility to push this agenda forward, in legislative consultations, courtrooms, regulatory proceedings, and continental forums where the rules of the AI era are still being written.

The title of this paper borrows language from a participant at an African AI governance forum who warned that Africa must choose between being a standard maker and a standard taker in the global AI governance conversation. That choice is not yet made. The window in which it can be made on Africa's terms remains open, but it will not remain open indefinitely. The EU AI Act is already in force. Global AI governance standards are crystallising. Foreign technology companies are already deploying AI systems across the continent under legal frameworks written for other places and other priorities. Every month that passes without binding African AI legislation is a month in which the terms of Africa's

⁷⁷ Marketing Edge Nigeria, 'Why Your Marketing AI Just Became a Data Protection Problem' (Marketing Edge, March 2026) <https://marketingedge.com.ng/why-your-marketing-ai-just-became-a-data-protection-problem-and-what-nigerian-brands-must-do-now/> accessed 30 July 2026.

⁷⁸ Opportunities for Youth, 'Apply Now: Africa AI Policy Fellowship 2026 for Legal, Policy and Tech Professionals' (Opportunities for Youth, March 2026) <https://opportunitiesforyouth.org/2026/03/23/apply-now-africa-ai-policy-fellowship-2026-for-legal-policy-and-tech-professionals/> accessed 30 July 2026.

digital future are being set by others. The legal profession needs to understand that urgency, and to act accordingly. Africa's AI future is too important to be left to technologists and strategists alone. It needs lawyers, and it needs them now.