CENTER FOR FISCAL TRANSPARENCY AND PUBLIC INTEGRITY

POLICY ARTICLE ON

ARTIFICIAL INTELLIGENCE

GOVERNANCE FRAMEWORK IN NIGERIA

EXECUTIVE SUMMARY

Artificial Intelligence (AI) is already transforming key sectors in Nigeria, including banking, healthcare, education, agriculture, and public governance, despite the absence of a binding regulatory framework. Stakeholder consultations on Nigeria's AI Governance Framework revealed that while the country has adopted important policy commitments, these have not translated into enforceable legal and institutional safeguards. AI deployment is expanding rapidly. Nigerian banks now use AI-powered customer service systems, while the Central Bank of Nigeria has integrated AI into Anti-Money Laundering compliance processes. Yet citizens lack legal protections such as rights to transparency, explanation, or redress against harmful automated decisions. Although the National Artificial Intelligence Strategy (2024) presents an ambitious vision for ethical and innovative AI development, stakeholders noted major implementation gaps, including the absence of funding structures, timelines, measurable targets, and clearly assigned institutional responsibilities. At the same time, Nigeria faces rising AI-related risks, including deepfake scams, AI-generated non-consensual content, and misinformation that threaten public trust, electoral integrity, and social cohesion. These challenges are worsened by weak accountability mechanisms for digital platforms operating in Nigeria. Structural constraints such as inadequate electricity supply, low internet penetration, limited research capacity, and insufficient AI talent further complicate Nigeria's AI ambitions. However, these limitations make effective governance even more urgent, as unregulated AI disproportionately harms vulnerable and digitally excluded populations. This policy brief, therefore, calls for Nigeria to move beyond policy aspirations toward a rights-based, context-sensitive, and enforceable AI governance framework that protects citizens, promotes responsible innovation, and strengthens national capacity in the evolving global AI landscape.

BACKGROUND AND POLICY CONTEXT

Artificial Intelligence has moved rapidly from a conceptual policy discussion to a practical governance challenge in Nigeria. As documented during the Assessment of the Artificial Intelligence Governance Framework in Nigeria, AI systems are already embedded in everyday institutional decision-making, often without public awareness or legal safeguards. Stakeholders repeatedly emphasised that Nigeria is not debating a future technology; it is grappling with a present reality unfolding faster than its governance architecture can respond to.[1]

During the keynote address, it was noted that AI deployment in Nigeria spans multiple high-impact sectors. In the financial sector alone, "as of February 2024, thirteen deposit money banks had integrated AI-powered chatbots into customer service operations," while by 2026, "the Central Bank of Nigeria formally incorporated AI into its Anti-Money Laundering compliance framework." These systems influence the customer access to services, fraud detection, transaction monitoring and compliance regulation outcomes.[2] Similar patterns were observed in healthcare, where AI diagnostic tools have been piloted in teaching hospitals; in agriculture, employing precision farming technologies; and in education, via automated learning platforms. Yet across all these sectors, AI systems are being deployed before any binding statutory standards governing transparency, accountability, or citizen redress.

Nigeria's policy response to this reality has been significant but incomplete. The National Artificial Intelligence Strategy (2024) represents the most comprehensive articulation of the country's AI ambition to date. According to stakeholders, the strategy is "a well-crafted document built around five bold goals," including foundational infrastructure development, ecosystem growth, ethical AI aligned with Nigerian values, and the establishment of a dedicated governance framework with a specialised regulatory body.[3] Nigeria's international positioning has also strengthened: the country climbed 31 places to 72nd in the 2025 Oxford Government AI Readiness Index, up from 103rd in 2023, and co-sponsored the United Nations General Assembly's first AI resolution in 2024.[4] These developments demonstrate political recognition of AI's importance.

However, as multiple contributors have stressed, policy momentum has not translated into enforceable governance. The strategy does not specify when

governance institutions will be created, how they will be funded, or how progress will be measured. One panellist drew a sharp comparison with Rwanda's AI strategy, which includes an explicit budget of approximately $76.5 million, a defined five-year implementation window and built-in evaluation mechanisms. Nigeria's approach, by contrast, was described as “ambition without the implementation architecture to match it”.[5] This lack of timelines, key performance indicators and designated responsibility creates a governance vacuum in which AI systems continue to expand unchecked.

The legislative landscape reflects a similar pattern. Nigeria currently has no binding AI law. Bills introduced in 2021 and 2023 failed to complete the legislative cycle, leaving AI governance fragmented across sector-specific regulations. The National Digital Economy and E-Governance Bill (2025), currently awaiting presidential assent, represents the most consequential opportunity to date.[6] Stakeholders highlighted that the bill proposes risk-based classification of AI systems, mandatory algorithmic transparency, annual audits for high-risk deployments, accreditation of AI auditors, and enforceable penalties for non-compliance. Yet concerns were raised that the bill is reportedly modelled on the European Union AI Act, even as the EU itself is retreating from that framework amid fears it stifles innovation. This raises critical questions about whether Nigeria's governance approach is being designed for its own context or borrowed wholesale from jurisdictions with vastly different infrastructural and economic realities.

Compounding these challenges is deep regulatory fragmentation. At least nine regulatory bodies currently exercise overlapping jurisdiction over AI deployment, including the National Information Technology Development Agency (NITDA), the Nigeria Data Protection Commission (NDPC), the Central Bank of Nigeria (CBN), the Nigerian Communications Commission (NCC), and the Federal Competition and Consumer Protection Commission (FCCPC). As noted during the dialogue, there is “no formal coordination mechanism between them,” creating enforcement gaps and institutional confusion. In such an environment, accountability for AI-related harms is easily diffused, allowing violations to persist without clear responsibility or remedy.

The limitations of existing data protection frameworks further expose this gap. While the Nigeria Data Protection Act 2023 governs personal data, stakeholders emphasised that it[7] “addresses what happens to data, not what AI systems do with it.” AI profiling, automated decision-making, and algorithmic bias largely fall outside its enforcement scope. This is particularly concerning, given that the Nigeria Deposit Insurance Corporation flagged algorithmic bias as a governance risk in 2024, yet no mandatory bias-mitigation or audit standards have been

introduced. As a result, citizens affected by discriminatory or erroneous automated decisions currently have no AI-specific legal recourse.

Profound structural constraints also shape Nigeria's AI governance challenge. Global data presented during the dialogue showed that electricity consumption from AI data centres already amounts to approximately 415 terawatt-hours annually, growing at about 12 per cent per year.[8] Nigeria, by comparison, produces a fraction of this output, with chronic power shortages undermining even basic digital infrastructure. Bridging the electricity gap to support meaningful AI development would require an estimated $10 billion annually for ten years, a scale of investment that has not been integrated into current planning. Internet penetration remains uneven, ranging from 34 to 54 per cent, while Africa accounts for less than 1 per cent of global research output. These realities define Nigeria's position at the margins of the global AI value chain.[9]

Despite these constraints, stakeholders strongly rejected the notion that Nigeria should abstain from AI governance because it has not developed the technology. As one participant argued, Nigeria already regulates pharmaceuticals it does not manufacture; AI should be no different. The real question, repeatedly posed during the discussions, is whether Nigeria will shape how AI functions within its borders or remain subject to external commercial and geopolitical interests. This policy document calls for an urgent shift from abstract strategy to enforceable safeguards.

AI-Enabled Harms and Emerging Risks to Nigerian Citizens

The absence of enforceable AI governance in Nigeria is not an abstract regulatory concern; it is already causing measurable, escalating harm to citizens. Throughout the stakeholder dialogue and governance assessment, participants consistently emphasised that AI-enabled risks are no longer hypothetical. They are materialising in ways that undermine financial security, personal dignity, public trust, and democratic stability. Civil society organisations, therefore, argue that AI governance must be grounded first and foremost in the lived experiences of Nigerian citizens, particularly those most vulnerable to digital abuse.

One of the most visible and documented categories of harm discussed during the event is AI-enabled fraud and impersonation. Stakeholders cited multiple instances of highly convincing deepfake videos and audio recordings impersonating prominent Nigerian business leaders that were circulated to lure unsuspecting citizens into financial scams. As one contributor noted, these deepfakes are no longer crude fabrications but “so sophisticated that they are virtually indistinguishable from authentic content.” Victims of these scams often lose life savings, yet there is currently no AI-specific legal mechanism that

compels platforms to act swiftly or provides victims with meaningful redress.

Closely linked to this is the rapid expansion of AI-driven misinformation and disinformation. What began as casual image manipulation for entertainment has evolved into a systematic ecosystem in which false narratives are deliberately engineered and amplified at scale. Participants warned that AI tools now enable bad actors to generate misleading videos, images, and text in volumes that overwhelm traditional fact-checking mechanisms. This phenomenon poses risks in Nigeria's already fragile information environment, where misinformation has historically fueled ethnic tension, electoral disputes, and communal violence. Civil society representatives stressed that without governance safeguards, AI could become a force multiplier of instability.

Perhaps the most disturbing harms documented during the dialogue relate to gender-based digital abuse. The African Centre for Information Integrity presented evidence that AI tools on the platform X (formerly Twitter), including generative systems such as Grok, are being used to create non-consensual sexualised images of women by uploading real photographs and instructing the system to manipulate them. These images are then circulated publicly, causing profound reputational, psychological, and social harm to victims. Despite repeated reports to the platform, responses have been minimal, with responsibility deflected by framing complaints as privacy disputes involving content creators rather than violations against the victims. Stakeholders described this pattern as a clear illustration of why platform self-regulation is insufficient in the AI era.

Beyond platform-based abuse, participants raised alarm over the exploitation of vulnerable populations, particularly in rural and low-income communities. Youth advocates highlighted applications that actively incentivise users to photograph individuals without their knowledge or consent and to upload such content for monetisation or engagement. These images are later repurposed for scams, fabricated narratives, or misleading fundraising campaigns. As one NYSC participant observed, people in digitally marginalised communities often lack both awareness and legal recourse, making them disproportionately exposed to AI-enabled exploitation. In such contexts, the absence of governance does not produce neutrality; it entrenches inequality.

AI-driven harms are also emerging within public- and private-sector decision-making systems, where opacity compounds risk. Automated systems used in banking, taxation, procurement, and service delivery can replicate or intensify existing social biases. The Nigeria Deposit Insurance Corporation's 2024 warning on algorithmic bias was cited as a critical red flag, yet no mandatory standards for

bias testing or disclosure exist. Citizens denied loans, flagged for fraud, or excluded from public benefits by automated systems have no guaranteed right to understand how those decisions were made or to challenge them. This creates what one participant described as a “black box governance” problem, where power is exercised without accountability.

A recurring theme throughout the discussions was that platform companies are the primary vectors through which AI-enabled harm reaches Nigerian citizens, yet they operate with minimal enforceable obligations. While Nigeria has demonstrated its capacity to assert regulatory authority, most notably through its lawsuit against Meta, which was ultimately settled for approximately $32 million, stakeholders stressed that such actions remain episodic rather than systemic.[10] Without clear statutory duties for content moderation, algorithmic accountability, and user protection, platforms retain disproportionate power over Nigeria's digital public sphere.

Importantly, participants rejected the argument that these harms are inevitable side effects of innovation. Instead, they framed them as the predictable outcome of deploying powerful technologies without guardrails. One panellist drew an analogy to aviation safety, noting that aircraft accidents are rare not because planes are simple, but because regulation, oversight, and accountability are embedded at every stage of design and operation. In contrast, AI systems in Nigeria are being deployed into society without comparable safety architecture, despite their capacity to affect millions simultaneously.

Participants therefore contend that the documented harms outlined above provide a clear evidentiary basis for urgent governance action. These are not isolated incidents but interconnected manifestations of a systemic failure to regulate power, protect rights, and assign responsibility in the AI ecosystem. Left unaddressed, these harms will deepen public mistrust in digital systems, exacerbate social divisions, and erode confidence in both government and technology.

Institutional, Legal, and Regulatory Deficiencies in Nigeria's AI Governance Architecture.

The harms documented in the preceding section are not occurring in a vacuum; they are the direct consequence of deep and persistent institutional, legal and regulatory deficiencies in Nigeria's AI governance architecture. Throughout the stakeholder dialogue, contributors repeatedly returned to a central diagnosis: Nigeria's AI challenge is not a lack of vision, but a failure of institutionalisation. Policies exist, conversations are active, and international commitments have

been made, yet the structures needed to translate intent into protection remain largely absent.

At the legal level, Nigeria currently lacks a binding AI-specific statute. While multiple AI-related bills have been introduced since 2021, none have completed the legislative cycle. As a result, AI deployment in Nigeria is indirectly governed by a patchwork of sectoral laws that were not designed to address algorithmic decision-making, automated profiling, or systemic AI risks. Stakeholders described this situation as one in which "AI systems are influencing public and private decisions without any dedicated legal authority overseeing how those decisions are made, tested, or challenged." This absence of statutory clarity creates uncertainty for institutions, developers, regulators, and citizens alike.

The National Digital Economy and E-Governance Bill (2025) represent the most promising attempt to close this gap.[11] Participants noted that the bill introduces several critical governance tools, including risk-based classification of AI systems, mandatory algorithmic transparency, audit requirements for high-risk use cases, accreditation of AI auditors, and enforceable penalties for non-compliance. However, concerns were raised on two fronts. First, the bill remains unassented, leaving its future uncertain. Second, its reported modelling on the European Union AI Act raises questions about contextual suitability. As one contributor cautioned, Nigeria risks importing a regulatory model from a region that is itself reassessing its approach due to innovation constraints, rather than developing a framework calibrated to Nigeria's infrastructural, economic, and institutional realities.

Institutionally, Nigeria's AI governance landscape is characterised by fragmentation and overlapping mandates. At least nine regulatory bodies currently exercise some degree of authority over AI deployment, including the National Information Technology Development Agency (NITDA), the Nigeria Data Protection Commission (NDPC), the Central Bank of Nigeria (CBN), the Nigerian Communications Commission (NCC), and the Federal Competition and Consumer Protection Commission (FCCPC). Each operates within its own statutory remit, yet AI systems routinely cut across these boundaries. As highlighted during the discussions, there is "no formal coordination mechanism" among these bodies, resulting in regulatory blind spots where AI-related harms fall through the cracks.

This fragmentation is particularly problematic in high-stakes sectors such as finance, telecommunications, and public administration, where AI systems simultaneously implicate data protection, consumer rights, competition law, and sector-specific regulation. Without a coordinating authority or formal inter-

agency framework, enforcement becomes inconsistent and reactive. Civil society participants warned that this environment incentivises regulatory arbitrage, allowing powerful actors to exploit ambiguity while ordinary citizens bear the consequences.

A further structural gap lies in the absence of an independent AI regulatory authority. Although the National Artificial Intelligence Strategy explicitly proposes establishing a specialised AI governance body, no such institution currently exists. NITDA has assumed a de facto leadership role. Still, stakeholders noted that it lacks an explicit AI mandate and lacks independent enforcement powers commensurate with the scale of the challenge. One panellist observed that "leading is not the same as regulating," underscoring the difference between policy coordination and legally grounded oversight. Without an independent regulator, AI governance remains administratively weak and politically vulnerable.

The limitations of Nigeria's data protection regime further expose regulatory inadequacies. While the Nigeria Data Protection Act 2023 provides an important foundation for personal data governance, it was not designed to address AI-specific risks. As repeatedly emphasised during the dialogue, the Act governs "what happens to data, not what AI systems do with it." Automated decision-making, algorithmic profiling, and systemic bias largely fall outside its explicit scope. This gap persists despite warnings from the Nigeria Deposit Insurance Corporation in 2024 that algorithmic bias constitutes a material risk to financial stability and consumer protection. The absence of mandatory bias audits, impact assessments, or explainability requirements leaves citizens unprotected against discriminatory or erroneous automated outcomes.

Another critical gap identified is the lack of procedural rights for citizens affected by AI systems. There is currently no statutory right to explanation, no guaranteed access to algorithmic reasoning, and no clear appeals process for individuals harmed by automated decisions in either the public or private sector. Participants described this as a fundamental failure of accountability, noting that governance systems lose legitimacy when decisions affecting livelihoods, access to services, or reputations cannot be questioned or understood.

Beyond formal institutions, stakeholders also highlighted deficiencies in technical and enforcement capacity. Even where regulators possess nominal authority, they often lack the technical expertise, resources, and tools required to audit complex AI systems. This capacity gap is exacerbated by Nigeria's broader infrastructural constraints, including unreliable electricity, limited access to high-performance computing, and a shortage of AI specialists within the public

sector. Without deliberate investment in regulatory capacity, even well-designed laws risk becoming symbolic rather than effective.
Civil society organisations further noted the absence of formal roles for non-state actors within Nigeria's AI governance framework. There are no institutionalised mechanisms for independent monitoring, civil society audits, or community-based reporting of AI harms. Youth, despite being both the largest user base and a growing segment of AI developers, remain largely excluded from decision-making processes. As one participant stated, “governance without participation is enforcement without legitimacy.” This exclusion undermines transparency and weakens public trust.

Structural and Infrastructure Constraints Shaping Nigeria's AI Governance Choices.

Throughout the stakeholder dialogue, participants consistently warned against treating AI governance as a purely legal or technical process separated from Nigeria's material conditions. Instead, they emphasised that energy, connectivity, research capacity and economic structure are not peripheral issues; they are determinative constraints that must inform governance choices.
The most fundamental of these constraints is the energy infrastructure. AI systems, notably those involving large-scale data processing, cloud computing and data centres, are among the most energy-intensive technologies in the modern economy. Data presented during the dialogue cited findings of the International Energy Agency, indicating that electricity consumption by AI data centres already amounts to approximately 415 terawatt-hours annually and is growing at an estimated 12 per cent per year. Nigeria's total electricity production, however, remains dramatically lower, with persistent instability, transmission losses and access gaps. As one participant bluntly pointed out, “Nigeria simply does not have the energy infrastructure to support the development of data centres at scale.”

The gap is not marginal. One estimate found that to bridge Nigeria's electricity deficit to a level capable of supporting serious AI development, the country would need to invest approximately $10 billion annually for 10 years for a cumulative $100 billion commitment.[12] Without such investment, aspirations for data localisation, sovereign AI infrastructure, or large-scale domestic model training remain largely rhetorical. Civil society organisations argue that AI administrative frameworks that assume the availability of stable, high-capacity power infrastructure risk being detached from reality and therefore ineffective.

Closely linked to energy is the challenge of digital connectivity. Internet penetration in Nigeria ranges from 34 to 54 per cent, depending on the methodology used, with disparities between urban and rural areas. Large

segments of the population remain entirely offline, while others rely on expensive, unreliable connections. Stakeholders from development organisations stressed that discussions about AI deployment and governance often overlook that many communities lack even basic internet access. In such contexts, AI risks deepening existing inequalities by concentrating benefits among already connected populations while excluding or exploiting those on the margins.
Another structural constraint repeatedly highlighted is Nigeria's position in the global AI value chain. Participants mapped the AI ecosystem from the semiconductor manufacturing and cloud infrastructure through core models and application layers. Nigeria's current innovation activity exists almost exclusively at the application layer, while remaining entirely dependent on foreign infrastructure at every layer below it. Semiconductors, large-scale cloud services, training computers, and even core datasets are controlled by external actors. One private sector contributor described this as a form of “stack dependency” that severely limits Nigeria's bargaining power and self-governance within the AI ecosystem.

Weaknesses in research and knowledge production compound this dependency. Less than 1% of global research and scientific output originates from Africa, and Nigeria's contribution remains modest even within that context. Participants noted that advanced AI development is closely tied to sustained investment in universities, research institutions, and interdisciplinary knowledge production, areas where funding remains chronically inadequate. Without addressing this deficit, Nigeria risks remaining a consumer rather than a shaper of AI systems, regardless of regulatory ambition.

Human capital constraints further complicate the picture. Stakeholders cited data indicating that 9 out of 10 African businesses report AI skills shortages, and that Nigeria currently lacks a national AI reskilling or workforce transition policy. While Nigerian technologists are developing innovative solutions, particularly in fintech and health technology, the lack of structured talent pipelines hampers scalability and sustainability. Moreover, public sector institutions, those most responsible for governance, often lack in-house technical expertise to audit, interrogate, or enforce AI systems. This creates a paradox in which regulators are tasked with overseeing technologies they may not fully understand.

Economic structure also shapes governance choices. Nigeria's fiscal space is constrained, with competing priorities across health, education, security, and infrastructure. Participants referenced the estimated $78–$100 million cost of training a single major foundational AI model, such as GPT-4, noting that such expenditures are difficult to justify within Nigeria's current budgetary realities. Civil society organisations caution that governance frameworks should not

assume that Nigeria can or should replicate the AI development trajectories of the United States or China. Instead, governance must focus on risk management, accountability, and the protection of the public interest, even in a context of technological dependence.

Importantly, several contributors warned against misinterpreting these constraints as arguments for abstaining from governance. On the contrary, they argued that structural weakness increases, rather than reduces, the need for governance. In environments with limited infrastructure, low digital literacy, and high inequality, unregulated AI systems can cause disproportionate harm. As one participant observed, "unregulated AI in a structurally constrained environment concentrates harm among those least able to protect themselves."

Civil Society, Youth, And Citizen Participation in AI Governance

A consistent and compelling theme across the stakeholder dialogue was the recognition that Nigeria's AI governance challenge is not only institutional but democratic. Participants repeatedly warned that governance frameworks designed without meaningful citizen participation risk becoming technocratic exercises that fail to reflect lived realities or command public trust. Civil society organisations, therefore, assert that inclusive participation is not an optional add-on to AI governance; it is a core requirement for legitimacy, effectiveness, and justice.

At present, civil society and youth are largely positioned as observers rather than actors in Nigeria's AI governance process. Despite civil society organisations being at the forefront of documenting digital harms, advocating for data protection, and holding platforms accountable, there is no formal mechanism to embed them within AI oversight structures. As noted during the assessment, "there is no institutionalised role for independent civil society monitoring, auditing, or reporting of AI systems deployed in public sector functions." This exclusion weakens accountability and leaves governance overly dependent on state and corporate actors whose incentives may not align with the protection of citizens.

Youth exclusion is particularly troubling given Nigeria's demographic realities. Young people constitute the majority of Nigeria's population and are simultaneously the primary users, targets, and, increasingly, builders of AI systems. Yet, as several participants observed, youth engagement is often reduced to tokenistic consultation rather than structured participation. One NYSC corps member articulated this gap powerfully, arguing that Nigeria is failing to deploy young people as "changemakers and whistleblowers" in the digital

space, leaving them vulnerable to exploitation or misinformation. From a civil society perspective, this represents a profound missed opportunity.

Participants stressed that citizen awareness is a prerequisite for regulation. As one youth advocate stated during the dialogue, *"If there is no information, there can be no regulation."* Many Nigerians remain unaware that AI systems influence decisions about loans, employment screening, content moderation, and access to public services. This information asymmetry disempowers citizens and undermines democratic oversight. Civil society organisations argue that AI governance frameworks must therefore incorporate public education as a governance function, not merely a communications exercise.

An additional critical participation gap is the lack of accessible reporting and redress mechanisms for AI-related harm. Victims of deepfakes, non-consensual image manipulation, algorithmic discrimination, or automated exclusion have no dedicated, safe channels to report harm without fear of retaliation or stigma. Participants recommended creating an anonymous digital reporting platform for citizens to flag harmful machine-generated content or decisions. Such a platform, contend civil society organisations, would not only empower victims but also generate important data for regulators and decision-makers.

Civil society actors also highlighted the importance of independent monitoring and oversight. Without external scrutiny, AI governance risks being captured by institutional self-interest or corporate influence. Participants called for mechanisms that allow civil society organisations to conduct independent audits, publish shadow reports, and participate in oversight committees. These functions are particularly vital in high-risk public-sector deployments, where AI systems influence taxation, procurement, social benefits, and security decisions. Embedding civil society within governance structures would strengthen transparency and deter abuse.

The dialogue further underscored the need to recognise community-level realities. Development practitioners pointed out that discussions about AI governance often assume a baseline of digital access and literacy that does not exist in many rural or marginalised communities. Civil society organisations working at the grassroots level are uniquely positioned to surface these realities, yet their insights are rarely integrated into national policy design. Effective governance, participants argued, must be informed not only by technical expertise but also by social context.

Importantly, civil society organisations rejected the notion that participation slows innovation. Instead, they framed participation as a means of aligning

innovation with public interest. Governance systems that incorporate citizen voices are more likely to identify risks early, adapt to emerging harms, and maintain social legitimacy. In contrast, governance imposed from above risks backlash, non-compliance, and erosion of trust. As one participant observed, "governance without participation is enforcement without consent."

From a rights-based perspective, participation is also a matter of equity. AI systems often reproduce existing power imbalances unless deliberately countered. Women, persons with disabilities, rural populations, and economically marginalised groups are disproportionately affected by opaque automated systems and platform abuse. Civil society organisations argue that inclusive governance must therefore prioritise the voices of those most affected, rather than defaulting to elite or technocratic perspectives.

Strategic Positioning – Why Governance Cannot Wait?

As Nigeria approaches a decisive moment in its digital transformation, the question before policymakers is no longer whether Artificial Intelligence will shape the country's future, but who will shape how it does so. The stakeholder dialogue made clear that Nigeria already lives with the consequences of AI adoption without governance. Automated systems influence access to finance, shape information ecosystems, mediate general trust and amplify harm, all while operating largely outside the reach of enforceable legal and institutional control.
A central debate that emerged during the dialogue concerned the sequencing of innovation and regulation. One school of thought argued that Africa risks becoming the only region attempting to regulate a technology it did not develop, warning that premature regulation could entrench dependency and stifle innovation. This perspective highlighted Nigeria's weak position in the global AI value chain, where compute capacity, foundational models, and infrastructure are expected to remain concentrated in the United States and China for the next decade.

However, an equally compelling counterargument was advanced: Nigeria already regulates pharmaceuticals, aviation, telecommunications, and financial systems; it does not manufacture them. Governance, in this view, is not contingent on domestic production, but on territorial impact and public risk. As one participant argued, the real danger lies not in regulating too early, but in governing too late, after harm has become systemic and trust irreparably damaged.

From a civil society perspective, this debate must be resolved in favour of context-appropriate governance rather than abstention from governance. Nigeria does

not need to replicate the regulatory models of the European Union, the United States, or China. But neither can it afford a vacuum in which powerful technologies operate without accountability. Governance, properly understood, is not a barrier to innovation; it is the framework that determines whether innovation serves the public interest or entrenches inequality.

The dialogue also surfaced a critical geopolitical dimension. AI is increasingly recognised as a determinant of national power, economic competitiveness, and information sovereignty. Countries that fail to define how AI operates within their borders risk becoming passive sites of extraction, of data, attention, and value, without the capacity to shape outcomes. Nigeria's large population, market size, and digital footprint give it leverage, but only if translated into clear rules, enforceable standards, and institutional confidence.

Participants contend that Nigeria's strategic choice is not between innovation and regulation, but between deliberate governance and unmanaged exposure. In a context of infrastructural constraint, low digital literacy, and deep inequality, unmanaged AI does not remain neutral. It concentrates harm among women, young people, rural populations, and those least able to contest automated decisions or platform abuse. Governance delay is itself a political choice, with distributive consequences.

CONCLUSION

The stakeholder dialogue on AI governance in Nigeria revealed a rare moment of clarity and convergence. Across government, civil society, academia, the private sector, and youth constituencies, there was broad agreement on a central truth: Nigeria has a vision but lacks the mechanisms to translate that vision into protection, accountability, and public value.

The National Artificial Intelligence Strategy, international commitments, and rising global rankings signal ambition. But ambition without enforcement leaves citizens exposed. As one participant observed, “AI is already acting on Nigerians, even though Nigerians have no formal way to act back.” This asymmetry is the core governance failure that must now be addressed.

Civil society organisations issue this policy brief as both an affirmation and a warning. It affirms that Nigeria has the intellectual, institutional and social capacity to design an AI governance framework based on its own realities and values. It also warns that continued delay will allow harms to scale faster than remedies can, deepen public mistrust, and cede regulatory power to unaccountable corporate and external actors.

AI governance is not a future project. It is an urgent public accountability obligation. Nigeria must now move decisively from dialogue to decision, from strategy to statute, and from aspiration to safeguards.

POLICY RECOMMENDATIONS

1. Immediate enactment of binding AI legislation, including the prompt presidential assent to the National Digital Economy and E-Governance Bill, with all transparency, audit, and enforcement provisions preserved.

2. Establishment of an independent National AI Regulatory Authority, with a clear statutory mandate, enforcement powers, technical capacity, sustainable funding, and representation from civil society and technical experts.

3. Formal inter-agency coordination on AI governance, through a legally backed framework linking NITDA, NDPC, CBN, NCC, FCCPC, and other relevant regulators to prevent jurisdictional gaps and regulatory arbitrage.

4. Expansion of the mandate of the Nigeria Data Protection Commission to explicitly cover AI profiling, automated decision-making, algorithmic discrimination and mandatory impact and bias assessments for high-risk AI systems.

5. Introduction of citizen rights in automated decision-making, including the right to explanation, access to important review and clear appeal mechanisms for AI-driven outcomes in both the public and private sectors.

6. Mandatory platform accountability provisions, requiring digital platforms to rapidly remove harmful AI-generated content, cooperate with Nigerian regulators, and face enforceable penalties for repeated non-compliance.

7. Creation of an anonymous national reporting and whistleblowing platform for AI-related harm, accessible to citizens without fear of retaliation, stigma or technical barriers.

8. Institutionalisation of civil society monitoring and oversight roles, including independent audits, shadow reporting, and participation in AI governance bodies and scrutiny processes.

9. A national AI capacity and talent strategy covering public sector regulators, educators and developers, with targeted investment in Nigerian language datasets and locally relevant AI research.

10. Integration of AI governance with infrastructure planning, making sure that energy, broadband and digital inclusion policies are treated as basic components of a responsible AI deployment.

11. Structured youth participation in AI governance, including training NYSC members and young professionals as AI governance advocates, community educators, and digital accountability actors.

12. Adoption of a context-specific governance model, rejecting wholesale regulatory imports and instead designing AI rules calibrated to Nigeria's economic, infrastructural, and social realities.

REFERENCES

Centre for Fiscal Transparency and Public Integrity (CeFTPI). (2026).

Reflections on the Stakeholder Dialogue on Artificial Intelligence Governance Framework in Nigeria. Abuja: CeFTPI.

Centre for Fiscal Transparency and Public Integrity (CeFTPI) & Bureau of Public Service Reforms (BPSR). (2026). *Report on Assessment of the Artificial Intelligence Governance Framework in Nigeria. Abuja:* CeFTPI.

National Information Technology Development Agency (NITDA). (2024).

National Artificial Intelligence Strategy. Abuja: Federal Government of Nigeria.

Oxford Insights. (2025). *Government AI Readiness Index 2025*. Oxford: Oxford Insights Ltd.

United Nations General Assembly. (2024). *Resolution on the Promotion of Safe, Secure and Trustworthy Artificial Intelligence.* New York: United Nations.

International Energy Agency (IEA). (2024). *Energy and AI: Energy Demand from Data Centres, Artificial Intelligence and Cryptocurrency.* Paris: IEA.

Nigeria Data Protection Commission (NDPC). (2023). *Nigeria Data Protection Act.* Abuja: Federal Republic of Nigeria.

Nigeria Data Protection Commission (NDPC). (2023). *General Application and Implementation Directive (GAID)*. Abuja: NDPC.

Nigeria Deposit Insurance Corporation (NDIC). (2024). *Annual Report and Financial Stability Commentary.* Abuja: NDIC.

Central Bank of Nigeria (CBN). (2026). *Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Framework*. Abuja: CBN.

African Centre for Information Integrity (ACII). (2026). *Presentation on AI-Enabled Misinformation, Deepfakes, and Platform Accountability.* Stakeholder Dialogue, Abuja.

Federal Competition and Consumer Protection Commission (FCCPC). (2025).

Settlement Agreement with Meta Platforms Inc., Abuja: FCCPC.

Ministry of ICT and Innovation, Republic of Rwanda. (2024).

National Artificial Intelligence Policy and Implementation Framework. Kigali: Government of Rwanda.

McKinsey Global Institute. (2023). *The Economic Potential of Generative AI: The Next Productivity Frontier. New York:* McKinsey & Company.

World Bank Group. (2023). *Digital Economy for Africa (DE4A): Nigeria Country Diagnostic*. Washington, DC: World Bank.

[1] Centre for Fiscal Transparency and Public Integrity (CeFTPI), *Reflections on the Stakeholder Dialogue on Artificial Intelligence Governance Framework in Nigeria,* 16 April 2026

[2] Central Bank of Nigeria (CBN), *Anti-Money Laundering / Combating the Financing of Terrorism Regulatory Framework,* revised 2026.

[3] National Information Technology Development Agency (NITDA), *National Artificial Intelligence Strategy,* 2024.

[4] Oxford Insights, *Government AI Readiness Index 2025*.

[5] Rwanda Ministry of ICT and Innovation, *National Artificial Intelligence Policy and Implementation Framework,* 2024.

[6] National Information Technology Development Agency (NITDA), *National Artificial Intelligence Strategy,* 2024.

[7] Nigeria Data Protection Commission (NDPC), *Nigeria Data Protection Act,* 2023.

[8] International Energy Agency (IEA), *Energy and AI: Energy Demand from Data Centres, Artificial Intelligence and Cryptocurrency,* 2024.

[9] African Centre for Information Integrity (ACII), stakeholder presentation on AI-enabled misinformation and non-consensual image manipulation, April 2026.

[10] Meta Platforms Inc. settlement with the Federal Competition and Consumer Protection Commission (FCCPC) and Nigerian authorities, 2024–2025.

[11] Nigeria Data Protection Commission (NDPC), General Application and Implementation Directive (GAID), 2023.

[12] World Bank, Digital Economy for Africa Initiative: Country Diagnostics – Nigeria, latest available edition.

MISSION STATEMENT

To promote good governance, transparency, accountability and public sector integrity through advocacy.

OUR VISION

To enhance human dignity in the public space.

OUR FOCUS

- Fiscal Transparency
- Public Sector Integrity
- Access to Information
- Anti-Corruption
- Research
- Organi ed Crime Resilience Initiative
- Data Science

SUPPORTED BY
MacArthur Foundation

WWW.FISCALTRANSPARENCY.ORG