

Harmonising Innovation and Accountability: A Hybrid Legal Framework for Artificial Intelligence in Nigeria

A Comparative Constitutional and Regulatory Analysis

Prof. Osaretin George Izevbuwa, PhD, FICA

*Professor of Law and Deputy Vice-Chancellor (Administration), Igbiniedion University
Okada, Edo State, Nigeria*

isIzevbuwa.george@iuokada.edu.ng

Adesuwa Celestina Ogbeide, Esq. LLB, LLM

Legal Practitioner, Legal Technologist and AI Governance Researcher, Nigeria

Classicsacra64@gmail.com

Abstract

This article examined the legal and institutional problem of reconciling artificial-intelligence innovation with public accountability in Nigeria. It was motivated by the growing use of artificial intelligence in finance, agriculture, healthcare, education and public administration, notwithstanding the absence of a dedicated and fully operational statutory framework governing the technology as a distinct regulatory subject. The article adopted a doctrinal and comparative method. It analysed the Constitution of the Federal Republic of Nigeria 1999 (as amended), the Nigeria Data Protection Act 2023, the National Artificial Intelligence Strategy 2025 and relevant sectoral legislation. It then compared Nigeria's emerging approach with three deliberately selected models: the European Union's binding, risk-based regime; the United Kingdom's principles-led and sector-based approach; and Singapore's practical soft-law and assurance framework. The article argued that Nigeria should not transplant any one of these models wholesale. The authors maintained that the more appropriate course is a phased, constitutionally anchored hybrid framework which preserves room for socially beneficial innovation while imposing proportionate obligations on high-risk uses. In the immediate term, Nigeria should coordinate existing regulators, issue cross-sector AI principles, require impact assessments for high-risk systems, strengthen regulatory sandboxes and establish safeguards for public-sector deployment. In the medium term, the country should consolidate institutional capacity, clarify responsibility across the AI value chain and develop a Nigerian risk taxonomy. Binding AI legislation should follow when the State has sufficient technical and enforcement capacity to administer it effectively. The article concluded that innovation and accountability are not opposing ends: in Nigeria's circumstances, credible accountability is a condition for public trust, sustainable investment and enduring AI innovation.

1. Introduction

Artificial intelligence (AI) is no longer a speculative technology in Nigeria. It is increasingly used in credit assessment, fraud detection, customer service, diagnostic support, precision agriculture, recruitment, content generation and public-service delivery. Nigeria's National Artificial Intelligence Strategy (NAIS), published in September 2025, describes AI as a potentially transformative instrument for economic growth, social inclusion and technological advancement. It also recognises that the use of AI raises questions of privacy, fairness, transparency, accountability, human well-being and institutional competence.¹

The motivation for this investigation lies in the gap between the speed of adoption and the development of effective legal safeguards. The same system that improves access to credit may reproduce historical discrimination. A diagnostic tool may extend medical expertise to underserved communities but also generate unsafe recommendations if trained on unsuitable data. Automated decision-making may improve administrative efficiency while obscuring the reasons for decisions affecting employment, benefits, policing or access to essential services. Generative AI can reduce the cost of information and content production, yet also facilitate impersonation, fraud, deepfakes and disinformation.

This is fundamentally a problem of regulatory timing. Technology develops more quickly than legislation and public institutions, while intervention becomes more difficult after technologies and commercial practices have become entrenched.² At one end of the policy spectrum is precautionary regulation, which gives priority to avoiding serious or irreversible harm. At the other is permissionless innovation, under which experimentation should ordinarily proceed unless a compelling case of serious harm is established.³ Neither position, applied without qualification, is adequate for Nigeria. Premature and overly detailed regulation may impose costs that regulators cannot administer and local innovators cannot bear. Conversely, unrestricted experimentation may expose citizens to harms for which existing remedies are fragmented, slow or practically inaccessible.

The central question is therefore not whether Nigeria should choose innovation or accountability. It is how the legal system can promote beneficial AI development while ensuring that persons and institutions responsible for designing, deploying and using consequential systems remain answerable for their decisions and their effects. This question is especially important in a developing digital State confronting infrastructure deficits, limited

¹ Federal Ministry of Communications, Innovation and Digital Economy and National Information Technology Development Agency, *National Artificial Intelligence Strategy* (September 2025) 3–5 <https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf> accessed 21 July 2026 (NAIS).

² Larry Downes states the pacing problem as follows: 'Social, political, and economic systems change incrementally, but technology changes exponentially': Larry Downes, *The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age* (Basic Books 2009) 2. David Collingridge similarly observed: 'When change is easy, the need for it cannot be foreseen; when the need for change is apparent, change has become expensive, difficult and time-consuming': David Collingridge, *The Social Control of Technology* (Frances Pinter 1980) 11.

³ European Commission, *Communication from the Commission on the Precautionary Principle* COM (2000) 1 final. Adam Thierer defines permissionless innovation as the view that experimentation with new technologies and business models 'should generally be permitted by default': Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (rev edn, Mercatus Center 2016).

regulatory capacity, socio-economic inequality, linguistic diversity and dependence on models developed outside the country.

The article is deliberately centred on Nigeria. It examines the nature and scope of innovation and accountability in the Nigerian AI ecosystem; evaluates the constitutional, statutory and policy framework already in existence; and identifies the gaps that prevent that framework from operating as a coherent system. The comparative discussion is limited to the European Union, the United Kingdom and Singapore. These jurisdictions were selected because they represent three distinct but relevant regulatory techniques: binding risk-based legislation, principles-led sector regulation and practical soft-law assurance. The comparison is used to illuminate Nigeria's choices, not to displace Nigerian constitutional values or institutional realities.

2. Nature and Scope of Innovation and Accountability in the Introduction of Artificial Intelligence in Nigeria

2.1 The Innovation Imperative

Innovation, in the context of AI, extends beyond the creation of new software. It includes the development, adaptation and deployment of data-driven systems capable of producing predictions, recommendations, decisions or content. For Nigeria, its significance lies in the possibility of addressing persistent developmental constraints at scale. AI may improve agricultural forecasting and crop management; assist medical screening and resource allocation; support fraud detection and financial inclusion; enable adaptive learning; improve traffic and energy management; and make some public services faster and more accessible.

The economic case is substantial but must be stated with care. The NAIS projected that Nigeria's AI market could reach US\$434.4 million in 2026, reflecting rapid growth in adoption across finance, agriculture, healthcare and telecommunications.⁴ The Strategy also identified Nigeria's youthful population, entrepreneurial ecosystem and diaspora expertise as strategic assets. These advantages create an opportunity to develop products adapted to Nigerian languages, public institutions and market conditions rather than depending entirely on systems designed for different societies.

Innovation must therefore be understood broadly. It encompasses foundational infrastructure, research, local datasets, technical skills, commercialisation, public-private collaboration and the adaptation of existing models to Nigerian needs. The relevant policy objective is not merely to attract foreign AI products. It is to build national capacity to understand, test, improve and govern the systems upon which critical economic and public functions may increasingly depend.

2.2 The Meaning of Accountability

Accountability requires more than a general commitment to ethical conduct. It means that an identifiable person or institution must be responsible for an AI system throughout its life cycle; relevant decisions must be documented; foreseeable risks must be assessed and mitigated;

⁴ NAIS (n 1) 8–9. The figure is a projection reported in the Strategy and should not be read as a verified statement of actual market size in 2026.

affected persons must receive sufficient information; and effective avenues must exist for human review, complaint, redress and enforcement.

Several dimensions are involved. **Ex ante accountability** operates before deployment through data governance, testing, impact assessment, procurement standards and approval requirements. **Operational accountability** applies while a system is in use through monitoring, human oversight, incident reporting, security and record-keeping. **Ex post accountability** arises after harm through investigation, explanation, correction, compensation, administrative sanctions or judicial remedies. A credible framework must address all three.

Accountability is particularly necessary where AI systems influence rights, opportunities or access to essential services. A low-risk recommendation engine should not bear the same regulatory burden as facial-recognition surveillance, automated credit refusal, employment screening or diagnostic decision support. Proportionality therefore requires obligations to increase with the seriousness, scale and reversibility of the potential harm.

2.3 Innovation and Accountability as mutually Reinforcing Objectives

The relationship between innovation and accountability is sometimes presented as a contest in which regulation inevitably suppresses technological progress. That assumption is incomplete. Poorly designed regulation can certainly create unnecessary barriers, particularly for start-ups and researchers. However, the absence of clear responsibility can also inhibit adoption. Businesses, government agencies and members of the public are less likely to rely on systems whose accuracy, security and legal consequences cannot be evaluated.

Appropriate accountability can promote innovation by creating trust, clarifying expectations and preventing irresponsible actors from imposing costs on the wider ecosystem. The relevant distinction is therefore not between regulation and innovation, but between regulation that is proportionate, adaptive and administrable and regulation that is rigid, duplicative or disconnected from institutional capacity.

For Nigeria, a balanced framework must satisfy five considerations. First, it must be anchored in the Constitution and the protection of human dignity, privacy, fair hearing, expression and equality. Secondly, it must recognise the developmental value of experimentation, research and commercialisation. Thirdly, it must distinguish low-risk uses from systems capable of producing serious legal or material effects. Fourthly, it must be realistic about the technical and financial capacity of regulators and regulated entities. Finally, it must remain open to revision as evidence, technology and institutional competence evolve.

2.4 Nigerian context and limits of the Inquiry

Nigeria's circumstances make contextual regulation indispensable. Unequal internet access, inconsistent infrastructure, limited availability of high-quality local data and a shortage of specialised personnel affect both innovation and oversight. Systems trained mainly on foreign datasets may perform poorly across Nigeria's languages, accents, names, health profiles and social conditions. Historical data used in lending, recruitment or policing may reproduce existing patterns of exclusion. Dependence on foreign cloud services and foundation models also raises questions of data sovereignty, audit access and bargaining power.

The inquiry is therefore confined to the governance of civil, commercial and public-sector AI in Nigeria. It does not attempt a complete treatment of autonomous weapons, military intelligence or every field of robotics. Nor does it assume that every use of automated software should be regulated as high-risk AI. The focus is the legal architecture required where AI development or deployment may materially affect rights, safety, economic opportunity or public administration.

3. The Subsisting Legal Framework for Artificial Intelligence in Nigeria

Nigeria does not begin from a legal vacuum. The Constitution, the Nigeria Data Protection Act 2023 (NDPA), consumer-protection legislation and several sectoral instruments already apply to aspects of AI. The principal difficulty is that these rules were not designed as one integrated AI-governance system.

3.1 Constitutional Foundations

Chapter IV of the Constitution supplies the normative foundation of AI accountability. Section 34 protects the dignity of the human person and is relevant to dehumanising profiling, manipulative systems and uses that treat individuals merely as data points. Section 36 guarantees fair hearing in the determination of civil rights and obligations. It becomes important where an opaque automated process materially affects employment, credit, benefits, discipline or other interests without a meaningful opportunity to understand or challenge the outcome.⁵

Section 37 protects the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications. In *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission*, the Court of Appeal recognised that the constitutional protection of privacy extends to personal information and data.⁶ This provides a constitutional foundation for data protection, although not every breach of a statutory data rule necessarily constitutes an independent constitutional violation.

Section 39 protects freedom of expression and the press, interests implicated by content moderation, synthetic media and State responses to disinformation. Section 42 prohibits specified forms of discrimination and is relevant where algorithmic systems produce unequal outcomes linked to ethnicity, place of origin, sex, religion or political opinion. Section 45 permits certain restrictions that are reasonably justifiable in a democratic society, but it does not provide an unrestricted license for AI-enabled surveillance or other rights-limiting measures.⁷

The Constitution therefore sets substantive boundaries. It does not, however, provide the technical rules necessary for testing, documenting, monitoring and auditing AI systems. Those operational requirements must be supplied by legislation, regulation and institutional practice.

⁵ Constitution of the Federal Republic of Nigeria 1999 (as amended), ss 34 and 36.

⁶ Constitution, s 37; *Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission* (2021) LPELR-55623 (CA). See also N Orji, 'Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v NIMC: A Milestone towards a Human Right-Based Approach to Data Protection in Nigeria' (2022) 16(1) *The Nigerian Juridical Review* 306. ⁷ Constitution, ss 39, 42 and 45.

3.2 The Nigeria Data Protection Act 2023 and the General Application and Implementation Directive 2025

The NDPA is presently the most important statute directly applicable to data-intensive AI. Section 24 establishes principles of lawful, fair and transparent processing, purpose limitation, data minimisation, accuracy, storage limitation, security and accountability.

Section 25 identifies lawful bases for processing. Section 28 requires a data privacy impact assessment where processing is likely to result in high risk to the rights and freedoms of data subjects, while section 30 regulates sensitive personal data.⁷

Section 37 is especially significant. It restricts decisions based solely on automated processing, including profiling, where the decision produces legal or similarly significant effects, subject to statutory exceptions. It also preserves safeguards including human intervention, an opportunity for the data subject to express a view and a right to contest the decision.⁸ These protections can support AI accountability in credit, insurance, recruitment and other consequential settings.

The Nigeria Data Protection Act—General Application and Implementation Directive 2025 (GAID) provides further implementation guidance, including guidance relating to data privacy impact assessments.⁹ Together, the NDPA and GAID can support risk assessment, documentation, human review and responsible data governance.

Their reach is nevertheless limited. The NDPA is primarily concerned with the processing of personal data. It does not comprehensively regulate every safety risk, intellectual-property issue, consumer harm, competition concern or public-law consequence arising from AI. It also does not by itself establish a complete taxonomy of prohibited, high-risk and low-risk AI uses. Consequently, the NDPA should be treated as a central pillar of AI governance, not as a complete AI code.

3.3 NITDA, NCAIR and the National Artificial Intelligence Strategy 2025

The National Information Technology Development Agency (NITDA), established under the NITDA Act 2007, and the National Centre for Artificial Intelligence and Robotics (NCAIR) have played leading roles in national AI policy and ecosystem development.¹⁰ Their work reflects the promotional dimension of AI governance: research, infrastructure, talent, innovation and commercialisation.

The NAIS 2025 is the most comprehensive statement of Nigeria's national AI policy. It presents a five-year program built around three strategic objectives and five pillars: foundational infrastructure; a sustainable AI ecosystem; adoption and sector transformation; responsible and

⁷ Nigeria Data Protection Act 2023, ss 24, 25, 28 and 30.

⁸ Ibid, s 37. The Nigeria Data Protection Commission also identifies the right not to be subjected to automated decision-making among the rights available under ss 34–38 of the Act: Nigeria Data Protection Commission, 'Your Rights as a Data Subject' <https://www.ndpc.gov.ng/> accessed 21 July 2026.

⁹ Nigeria Data Protection Commission, *Nigeria Data Protection Act—General Application and Implementation Directive* (2025), including sch IV on data privacy impact assessment; NDPC, 'DIAL Seeks NDPC Partnership for Data Privacy Impact Assessments' (28 March 2025) <https://www.ndpc.gov.ng/2025/03/28/dial-seeks-ndpcpartnership-for-data-privacy-impact-assessments/> accessed 21 July 2026.

¹⁰ National Information Technology Development Agency Act 2007; National Centre for Artificial Intelligence and Robotics, 'About NCAIR' <https://ncair.nitda.gov.ng/> accessed 21 July 2026.

ethical AI development; and a robust governance framework.¹¹ It envisages national AI principles, an AI Ethics Expert Group, assessment tools, a risk-management framework and a respected AI governance regulatory body.¹²

The Strategy is important, but its legal character must be stated accurately. It is a policy and implementation framework, not a substitute for legislation. Its principles do not automatically create enforceable duties, private rights of action or offences. Moreover, proposed institutions require clear mandates, funding, independence and relationships with existing regulators before they can operate effectively. There is also a potential conflict where the same institution is expected both to promote rapid AI adoption and to enforce safeguards against the risks created by that adoption.

3.4 Sectorial and Cross-cutting Legislation

Several additional statutes apply to particular AI-related conduct. The Federal Competition and Consumer Protection Act 2018 addresses unfair, misleading and exploitative practices and may apply to deceptive AI products, unfair terms and abuses affecting consumers. The FCCPC's proceedings against Meta Platforms and WhatsApp demonstrate that existing consumer and data rules can support substantial enforcement against digital-market misconduct.¹³

The Cybercrimes (Prohibition, Prevention, etc.) Act 2015, as amended, applies to computer-related fraud, identity offences and unlawful access relevant to some AI-enabled misconduct. The Copyright Act 2022 may apply to unauthorised reproduction, training-data disputes and certain uses of protected works, although difficult questions remain concerning authorship, infringement and exceptions. The Nigeria Startup Act 2022 supports an enabling environment for technology enterprises. Financial regulators, including the Central Bank of Nigeria and the Securities and Exchange Commission, also possess sector-specific powers relevant to automated financial services, cyber security, sandboxes and robo-advisory services.¹⁴

This sectoral structure has an advantage: regulators understand the markets and activities within their mandates. Its weakness is fragmentation. The same system may engage data protection, consumer protection, financial regulation, equality, cybersecurity and administrative law. Without an agreed coordinating framework, businesses may face overlapping requirements while affected persons fall between institutional boundaries.

3.5 Material Gaps in the Existing Framework

Five gaps are particularly significant. First, no single binding framework classifies AI uses according to risk and assigns proportionate duties. Secondly, responsibility across the AI value chain remains uncertain: a harmful outcome may involve a foundation-model provider, local developer, data supplier, vendor and deploying institution. Thirdly, public-sector procurement

¹¹ NAIS (n 1) 3–5.

¹² Ibid 4 and 44–47.

¹³ Federal Competition and Consumer Protection Act 2018; Federal Competition and Consumer Protection Commission, 'Violations: Tribunal Upholds FCCPC's \$220 Million Fine Against Meta/WhatsApp' (25 April 2025) <https://fccpc.gov.ng/violations-tribunal-upholds-fccpcs-220-million-fine-against-meta-whatsapp/> accessed 21 July 2026.

¹⁴ Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended); Copyright Act 2022; Nigeria Startup Act 2022; Central Bank of Nigeria, *Regulatory Sandbox Operations Framework* (2021); Securities and Exchange Commission, *Rules on Robo-Advisory Services* (2021).

and deployment are not governed by a uniform AI impact-assessment and transparency regime. Fourthly, existing remedies may not address harms that do not depend on personal-data processing. Fifthly, enforcement capacity is uneven, especially where meaningful supervision requires access to models, data, logs and specialised technical expertise.

The legal system therefore contains substantial raw materials but lacks an organising framework. The appropriate response is not to discard existing law or create an entirely separate bureaucracy for every AI issue. It is to coordinate, extend and supplement the present framework in a manner proportionate to risk.

4. Discussion: Comparative Analysis of Three Selected Jurisdictions

Comparative analysis is useful only if the selected models are evaluated against Nigeria's constitutional values, developmental priorities and institutional capacity. The European Union, the United Kingdom and Singapore offer distinct approaches from which specific techniques may be adapted.

4.1 European Union: Binding and Risk-Based Regulation

Regulation (EU) 2024/1689, commonly known as the EU Artificial Intelligence Act, establishes a horizontal and binding regulatory framework. It prohibits specified practices regarded as unacceptable and subjects high-risk systems to requirements relating to risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity.¹⁵ It also imposes transparency obligations for specified AI interactions and synthetic content and establishes rules for general-purpose AI models.¹⁷

The principal strength of the EU model is differentiation by risk. It recognises that regulatory intensity should reflect the potential seriousness of harm rather than applying identical obligations to every AI system. It also places responsibility on providers and deployers and connects pre-deployment controls with post-market monitoring and enforcement.

For Nigeria, the transferable lesson is not the wholesale replication of the Act. The EU framework is extensive, technically demanding and supported by institutions with substantially greater resources. Direct transplantation could impose disproportionate compliance costs, discourage local experimentation and produce rules that exist on paper but cannot be supervised. Nigeria should instead adapt the core ideas of prohibited practices, defined high-risk uses, impact assessment, human oversight, documentation and effective redress. The categories and duties must be simplified and calibrated to Nigerian capacity.

4.2 United Kingdom: Principles-led and Sector-based Regulation

The United Kingdom's 2023 White Paper and its 2024 Government Response proposed a context-sensitive framework implemented through existing sector regulators. Five crosssector principles guide the approach: safety, security and robustness; appropriate transparency and

¹⁵ Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L 2024/1689, arts 5, 6 and 8–15. ¹⁷ Ibid, art 50 and ch V.

explainability; fairness; accountability and governance; and contestability and redress.¹⁶ The framework initially relied on non-statutory implementation while developing central functions for coordination, risk assessment and regulatory coherence.¹⁷

The strength of this model is institutional pragmatism. It permits financial, health, competition, data and communications regulators to apply common principles within their existing mandates. It can respond more quickly than a detailed statute and reduce the risk that a new central regulator duplicates sectoral expertise.

Its weakness is the possibility of inconsistency, regulatory gaps and uncertain enforceability. General-purpose systems may affect several sectors without fitting comfortably within the mandate of any one regulator. Principles may also provide insufficient protection if regulators lack powers, resources or a duty to act.

Nigeria can adopt the UK's use of common cross-sector principles, existing regulators and a central coordinating function. However, Nigerian implementation should not depend indefinitely on voluntary compliance. Where AI materially affects constitutional rights, safety or essential services, minimum duties must eventually be binding.

4.3 Singapore: Soft law, Organisational Governance and Assurance Tools

Singapore's Model AI Governance Framework adopts a practical and organisation- centered approach. It addresses internal governance structures, the appropriate level of human involvement in AI-augmented decision-making, operational management and communication with stakeholders.¹⁸ Its companion implementation materials and AI Verify initiative translate general principles into testing, documentation and self-assessment tools.¹⁹

The value of the Singapore model lies in its emphasis on usable governance rather than abstract declarations. Organisations are encouraged to assign responsibility, document system objectives, evaluate data and model risks, determine when human review is required and communicate material information to affected persons. Such practices can improve conduct before a comprehensive statute is enacted.

For Nigeria, soft-law tools can be deployed quickly through regulatory guidance, procurement requirements, professional standards and sandboxes. They are particularly suitable for building capacity among start-ups, public agencies and regulators. Their limitation is that voluntary frameworks may not deter powerful actors or provide adequate remedies after serious harm. They should therefore operate as the first layer of a phased system, supported by existing law and followed by binding rules for high-risk uses.

¹⁶ Department for Science, Innovation and Technology, *A Pro-Innovation Approach to AI Regulation* (CP 815, March 2023); Department for Science, Innovation and Technology, *A Pro-Innovation Approach to AI Regulation: Government Response to Consultation* (CP 1019, February 2024) paras 10–12.

¹⁷ Government Response (n 18) paras 16–20.

¹⁸ Infocomm Media Development Authority and Personal Data Protection Commission, *Model Artificial Intelligence Governance Framework* (2nd edn, 2020).

¹⁹ Personal Data Protection Commission, 'Second Edition of Model AI Governance Framework Now Available' (21 January 2020) <https://www.pdpc.gov.sg/news-and-events/announcements/2020/01/second-edition-of-modelai-governance-framework-now-available> accessed 21 July 2026; Infocomm Media Development Authority, *AI Verify*.

4.4 Comparative Synthesis and Application to Nigeria

The three models reveal that no single regulatory form is sufficient. The EU contributes a clear risk-based architecture and enforceable duties. The UK demonstrates how common principles can be applied through existing sector regulators, supported by central coordination. Singapore shows how governance can be operationalised through practical tools, testing and organisational responsibility.

Nigeria should combine these lessons in a hybrid framework. It should begin with common national principles and operational guidance implemented by the NDPC, NITDA, FCCPC and relevant sector regulators. High-risk systems should be identified through a Nigerian taxonomy focused on actual contexts of harm, including biometric identification, publicsector eligibility decisions, credit, employment, health, education admissions, policing and critical infrastructure. Such systems should be subject to impact assessment, documented human oversight, security testing, record-keeping and accessible challenge mechanisms.

At the same time, low-risk experimentation should remain comparatively unburdened. Regulatory sandboxes should offer supervised routes for testing innovative products, especially where the applicable law is uncertain. Small firms should receive templates, technical guidance and proportionate compliance pathways rather than being subjected immediately to the full burden designed for large or high-risk operators.

The framework must also remain African in orientation. The African Union's Continental Artificial Intelligence Strategy advocates an Africa-centred, development-focused approach grounded in inclusive growth, human rights, data governance and regional cooperation.²⁰ Nigeria should pursue interoperability with international markets without allowing foreign models to dictate domestic priorities or weaken constitutional protection.

5. Challenges and Prospects

5.1 Examination of the Glaring challenges

5.1.1 Institutional fragmentation and limited capacity

AI governance crosses the mandates of the NDPC, NITDA, FCCPC, sector regulators, lawenforcement bodies and public-procurement institutions. Overlapping powers can create inconsistent directives and forum disputes, while gaps may arise where every institution assumes another is responsible. Effective supervision also requires lawyers, data scientists, cybersecurity specialists, sector experts and investigators. Without sustained funding and technical capacity, even well-drafted rules will be difficult to enforce.

5.1.2 Infrastructure, data and skills constraints

Reliable electricity, broadband, cloud infrastructure, computing resources and high-quality data remain unevenly available. Local firms may be unable to test and document systems to the standard expected of global technology companies. Regulators face similar limitations. A compliance framework that ignores these realities may entrench foreign dominance rather than improve accountability.

²⁰ African Union, *Continental Artificial Intelligence Strategy* (July 2024)

<https://static.au.int/en/document/44004-doc-en-continentalaistrategyjuly2024pdf> accessed 21 July 2026.

5.1.3 Bias, exclusion and contextual mismatch

AI systems developed mainly with foreign datasets may not perform reliably across Nigeria's languages, accents, names, cultural practices and demographic characteristics. Historical Nigerian datasets may themselves contain discriminatory patterns. The problem is not resolved merely by collecting more data; lawful basis, quality, representation, security and purpose must also be addressed. The development of local-language resources and contextually appropriate evaluation benchmarks is therefore both an innovation policy and an equality measure.²¹

5.1.4 Opacity and the Accountability Gap

Modern AI supply chains divide control among model developers, data providers, vendors, integrators and deployers. The organisation interacting with an affected person may lack access to the underlying model, while the model provider may disclaim responsibility for the final use. Trade secrecy and technical complexity can further restrict explanation and audit. The result is a practical accountability gap in which harm is identifiable but legal and operational responsibility is dispersed.

5.1.5 Public-sector deployment and surveillance risk

Government use of AI deserves heightened scrutiny because the State exercises coercive power and determines access to public services. Automated systems used in policing, identity management, benefits, taxation, immigration or recruitment may affect large populations and constitutional rights. Procurement secrecy, vendor dependence and weak documentation can prevent meaningful review. Public-sector efficiency must therefore be pursued within a framework of legality, necessity, proportionality, transparency and human accountability.

5.1.6 Compliance cost and the risk of regulatory exclusion

Overly complex duties may favour large foreign firms capable of absorbing legal and technical costs while excluding local start-ups, universities and civic innovators. Proportionality requires simplified compliance routes, phased implementation and support tools. It does not justify exempting high-risk systems merely because their providers are small; the relevant question is the risk created, with the form and cost of compliance adjusted where possible.

5.2 Prospects under the Existing Legal and Institutional Framework

Nigeria has several foundations upon which a credible system can be built. The Constitution provides a rights-based standard. The NDPA contains principles, impact-assessment duties and protections relating to solely automated decisions. The GAID offers an implementation mechanism. Existing sector regulators have legal mandates, enforcement experience and knowledge of particular markets. The NAIS supplies a national vision that expressly includes responsible and ethical AI and a robust governance framework.

Enforcement activity in the digital economy also shows that Nigerian institutions are not wholly passive. In April 2025, the Competition and Consumer Protection Tribunal substantially upheld the FCCPC's findings and US\$220 million administrative penalty against Meta Platforms and

²¹ NAIS (n 1) 31–43; G Ayana and others, 'Decolonizing Global AI Governance: Assessment of the State of Decolonized AI Governance in Sub-Saharan Africa' (2024) 11(8) *Royal Society Open Science* 231994, doi:10.1098/rsos.231994.

WhatsApp following a joint investigation with the dataprotection authority.²² Although that matter did not establish a complete AI regime, it illustrates the capacity of existing law to address certain forms of digital-market misconduct.

Nigeria also possesses a large community of developers, researchers, technology enterprises and professionals. NCAIR's work on national AI capacity and local-language models indicates the possibility of building systems more responsive to Nigerian realities.²³ Universities, professional bodies and civil society can contribute independent research, testing, public education and scrutiny. Regulatory sandboxes already used in financial services provide an institutional model for supervised experimentation.

Regional cooperation is another prospect. Alignment with the African Union's continental strategy and relevant ECOWAS initiatives can reduce duplication, support cross-border standards and strengthen Nigeria's bargaining position in relation to multinational technology providers. Regional harmonisation should, however, preserve the higher protection available under the Nigerian Constitution and legislation.

5.3 Recommendations

5.3.1 Immediate Measures: Coordination, Guidance and Capacity

First, the Federal Government should establish an interim AI Governance Coordination Council through a legally appropriate instrument. Its membership should include the NDPC, NITDA/NCAIR, FCCPC, key sector regulators, public-procurement authorities, technical experts, academia, industry and civil society. Its purpose should be coordination and standard-setting, not the usurpation of existing statutory powers.

Secondly, the relevant regulators should jointly issue National Principles for Responsible AI. These should address safety and security; fairness and non-discrimination; transparency and explainability; privacy and data governance; human oversight; accountability; contestability and redress. Each regulator should explain how the principles apply within its statutory mandate.

Thirdly, the NDPC and NITDA should publish joint guidance on the application of sections 24, 28, 30 and 37 of the NDPA to AI systems. The guidance should include standard templates for AI and data-protection impact assessments, model and system documentation, incident records and human-review procedures. Guidance should distinguish personal-data obligations from wider AI risks so that the NDPA is not incorrectly presented as a complete AI statute.

Fourthly, all federal public institutions should be required to maintain a register of consequential AI systems. Before procurement or deployment, a public institution should complete an impact assessment addressing legal authority, purpose, data, accuracy, discrimination, security, necessity, proportionality, human oversight, vendor access and redress. A public summary should be released except to the extent that a lawful and specific ground of confidentiality applies.

Fifthly, sector regulators should expand coordinated AI sandboxes. Entry should not amount to immunity from existing law, but participating organisations should receive early regulatory

²² FCCPC (n 14).

²³ NCAIR (n 11). See also NAIS (n 1) 31–43.

guidance and a controlled environment for testing safeguards. Lessons from sandboxes should inform future rules and be published in anonymised form.

Finally, investment in regulatory capacity must accompany every new obligation. Training should combine law, data science, cybersecurity, audit and sector knowledge. Government should support local testing facilities, representative datasets, research grants and Nigerian language resources. Rules that require technical assurance without creating the capacity to provide or evaluate it will not succeed.

5.3.2 Medium-Term Measures: Risk Classification and Institutional Consolidation

Nigeria should develop a national AI risk taxonomy through public consultation. It should identify prohibited practices, presumptively high-risk uses and lower-risk applications. The classification should depend primarily on context, purpose, scale, affected population and severity of potential harm.

For high-risk systems, minimum obligations should include documented risk management; appropriate data governance; testing for accuracy, discrimination, robustness and security; technical records; meaningful human oversight; incident reporting; accessible notices; and a right to seek human review. Independent audit should be required where the scale or seriousness of risk warrants it.

Responsibility across the AI value chain should also be clarified. Contracts cannot be permitted to remove all responsibility from the actor best placed to prevent harm. Providers should be responsible for accurate documentation, known limitations and material changes within their control. Deployers should be responsible for lawful context, local testing, human oversight and the decisions ultimately made through the system. Where several actors contribute to a harm, the law should provide an intelligible basis for investigation and allocation of liability.

Institutional consolidation should follow evidence, not administrative fashion. If a dedicated AI body is established, its mandate must be clear, its independence protected and its relationship with the NDPC and sector regulators defined. Promotional and enforcement functions should be institutionally separated or protected by strong conflict-of-interest safeguards.

5.3.3 Longer-Term Measure: Lean, Rights-Protective Ai Legislation

Nigeria should enact dedicated AI legislation when the country has developed sufficient evidence, technical capacity and institutional coordination to administer it. The statute should be concise enough to remain adaptable and should avoid reproducing the EU AI Act in full.

At a minimum, the legislation should:

1. define the systems and actors within its scope;
2. prohibit narrowly specified practices incompatible with constitutional rights, including unjustified social scoring, manipulative systems causing serious harm and indiscriminate biometric surveillance;
3. identify high-risk contexts and prescribe proportionate duties;
4. guarantee notice, human review, contestability and accessible redress for consequential automated decisions;

5. assign responsibilities among providers, importers, vendors and deployers;
6. provide powers for investigation, audit, corrective orders and proportionate sanctions;
7. establish coordination among the competent regulators; and
8. provide periodic legislative and technical review.

Legislation should preserve research, open innovation and low-risk experimentation through proportionate exemptions or simplified pathways. However, no exemption should defeat constitutional rights or remove essential safeguards from a system merely because it is experimental.

5.4 Concluding Position

Nigeria need not choose between technological progress and legal accountability. The Constitution, the NDPA, the GAID, sectoral legislation and the NAIS already provide elements of a responsible framework. Their present weakness is fragmentation, uneven capacity and the absence of a coherent system for classifying risk and assigning responsibility.

The comparative analysis demonstrates that Nigeria should not copy a single foreign model. From the European Union, it should adopt proportionate risk classification and enforceable duties for high-risk systems. From the United Kingdom, it should adopt common principles implemented through existing sector regulators and supported by central coordination. From Singapore, it should adopt practical governance, testing and assurance tools capable of immediate use by organisations and regulators.

The appropriate Nigerian model is therefore a phased hybrid: soft-law principles, coordinated guidance, procurement safeguards, impact assessments and sandboxes in the immediate term; institutional consolidation, local testing capacity and a national risk taxonomy in the medium term; and lean, rights-protective legislation when effective administration becomes feasible. This approach does not postpone accountability. It uses existing constitutional and statutory powers immediately while building the capacity required for stronger and more specialised regulation.

Properly designed accountability is not an obstacle to innovation. It is the means by which innovation becomes trustworthy, investable and socially legitimate. Nigeria's long-term interest lies in an AI ecosystem that is not only productive, but also lawful, inclusive, explainable and answerable to the people whose lives it affects.

Bibliography Statutes, Regulations and International Instruments

- African Union Convention on Cyber Security and Personal Data Protection 2014.
- Constitution of the Federal Republic of Nigeria 1999 (as amended).
- Copyright Act 2022.
- Cybercrimes (Prohibition, Prevention, etc.) Act 2015 (as amended).
- Federal Competition and Consumer Protection Act 2018.
- National Information Technology Development Agency Act 2007.
- Nigeria Data Protection Act 2023, Act No 37 of 2023.
- Nigeria Data Protection Act—General Application and Implementation Directive 2025.
- Nigeria Startup Act 2022.
- Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1.
- Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L 2024/1689.

Cases

- Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v National Identity Management Commission* (2021) LPELR-55623 (CA).
- Meta Platforms Inc and WhatsApp LLC v Federal Competition and Consumer Protection Commission* (Competition and Consumer Protection Tribunal, 25 April 2025).

Books

- Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).
- David Collingridge, *The Social Control of Technology* (Frances Pinter 1980).
- Larry Downes, *The Laws of Disruption: Harnessing the New Forces that Govern Life and Business in the Digital Age* (Basic Books 2009).
- Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (rev edn, Mercatus Center 2016).

Journal Articles

- A Genus and A Stirling, 'Collingridge and the Dilemma of Control: Towards Responsible and Accountable Innovation' (2018) 47(1) *Research Policy* 61.
- N Orji, 'Incorporated Trustees of Digital Rights Lawyers Initiative & Ors v NIMC: A Milestone towards a Human Right-Based Approach to Data Protection in Nigeria' (2022) 16(1) *The Nigerian Juridical Review* 306.

G Ayana and others, 'Decolonizing Global AI Governance: Assessment of the State of Decolonized AI Governance in Sub-Saharan Africa' (2024) 11(8) *Royal Society Open Science* 231994.

Official and Institutional Sources

African Union, *Continental Artificial Intelligence Strategy* (July 2024).

Department for Science, Innovation and Technology (UK), *A Pro-Innovation Approach to AI Regulation* (CP 815, March 2023).

Department for Science, Innovation and Technology (UK), *A Pro-Innovation Approach to AI Regulation: Government Response to Consultation* (CP 1019, February 2024).

Federal Ministry of Communications, Innovation and Digital Economy and National Information Technology Development Agency, *National Artificial Intelligence Strategy* (September 2025).

Infocomm Media Development Authority and Personal Data Protection Commission (Singapore), *Model Artificial Intelligence Governance Framework* (2nd edn, 2020).

Infocomm Media Development Authority (Singapore), *AI Verify*.

Nigeria Data Protection Commission, *Nigeria Data Protection Act—General Application and Implementation Directive* (2025).