Quest Journals
Journal of Education, Arts, Law and Multidisplinary
Volume 16 ~ Issue 2 (Mar. – Apr. 2026) pp: 195-204
ISSN(Online): 2347-2895
www.questjournals.org

Research Paper

Artificial Intelligence Governance and Cybersecurity: Evaluating Nigeria's Legal and Regulatory Framework

KELVIN BRIBENA PhD[1]
Faculty of Law, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria

Abstract
Artificial intelligence is rapidly reshaping digital economies, public administration, financial services, health care, education, security, communications and commerce. In Nigeria, AI presents significant opportunities for innovation, public service delivery, fraud detection, financial inclusion, health diagnostics, agricultural productivity and national competitiveness. At the same time, AI systems generate serious legal and regulatory concerns, particularly in relation to privacy, data protection, cybersecurity, algorithmic accountability, discrimination, surveillance, misinformation, cybercrime, consumer protection and institutional coordination. This article evaluated Nigeria's legal and regulatory framework for AI governance and cybersecurity. It argued that Nigeria has built important legal foundations through the Constitution, the Nigeria Data Protection Act 2023, the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 as amended in 2024, the National Information Technology Development Agency Act (NITDA), sector-specific cybersecurity rules, the NITDA Code of Practice for online platforms, and the National Artificial Intelligence Strategy. However, the paper found that the framework remains fragmented and incomplete because Nigeria has not yet enacted a comprehensive AI governance statute that imposes binding lifecycle obligations on developers, deployers and users of high-risk AI systems. The paper employed the doctrinal research methodology evaluating the level of extant laws through primary and secondary sources respectively. It relied on the Constitution of the Federal Republic of Nigeria 1999 as amended, the Cybercrimes Act 2015 as amended, the Nigeria Data Protection Act 2023, the National Information Technology Development Agency Act as well as journal articles, declassified policy documents and other relevant online materials. The article concluded that Nigeria should adopt a risk-based AI governance model, strengthen cybersecurity-by-design obligations, harmonise institutional mandates, protect fundamental human rights, and develop enforceable standards for transparency, human oversight, impact assessment, auditability and incident reporting by moving from policy aspiration to enforceable governance.

Keywords: *Artificial Intelligence, Cybersecurity, Data Protection, AI Governance, Cybercrimes Act, NDPA, NITDA, Algorithmic Accountability, Digital Rights.*

I. Introduction

Artificial intelligence has become one of the defining technologies of the twenty-first century. It is no longer confined to laboratories or experimental research. AI now powers search engines, recommendation systems, fraud detection tools, biometric identification systems, credit-scoring models, automated customer service systems, generative content tools, predictive policing solutions, medical diagnostic tools, educational platforms, and cybersecurity systems. In Nigeria, AI is increasingly relevant to digital banking, fintech, telecommunications, e-commerce, public identity systems, health technology, legal technology, agriculture, taxation, security intelligence and electoral information ecosystems. The legal challenge is that AI systems do not merely process information; they can classify people, predict behaviour, generate persuasive content, automate decisions, amplify bias, and expose sensitive data to new forms of cyber risk.[2]

The governance of AI is therefore inseparable from cybersecurity. AI systems rely on large quantities of data, cloud infrastructure, application programming interfaces, software supply chains, model training

[1]Kelvin Bribena, LLB, BL, LLM, M.Sc, M.Ed, LLD, ACIArb, FNIMN, Head of Department, Jurisprudence and International Law, Faculty of Law, Niger Delta University, Wilberforce Island, Bayelsa State, Nigeria
[2]Organisation for Economic Co-operation and Development, *OECD AI Principles*<https://www.oecd.org/en/topics/sub-issues/ai-principles.html> accessed 24 June 2026

pipelines, user prompts, automated outputs and networked platforms. Each of these components can be attacked, manipulated or misused. Cybersecurity risks associated with AI include data poisoning, model inversion, prompt injection, adversarial attacks, unauthorised access, deepfake-enabled fraud, automated phishing, identity theft, malware generation, biometric spoofing, and large-scale disinformation campaigns.[3]Conversely, AI may also strengthen cybersecurity through anomaly detection, fraud monitoring, malware analysis, automated vulnerability discovery and incident response. The legal task is therefore twofold: to regulate AI as a source of risk and to enable AI as a tool for cyber resilience.

Nigeria's digital economy has grown significantly over the last decade. The country has an active fintech sector, a youthful population, expanding digital public infrastructure, increasing mobile penetration and a growing policy interest in emerging technologies. Yet the regulatory framework for AI remains at an early stage. Nigeria has adopted important laws and policy instruments relevant to AI, including the Nigeria Data Protection Act 2023, the Cybercrimes Act 2015 as amended in 2024, the National Information Technology Development Agency Act 2007, the NITDA Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries, the Nigeria Startup Act 2022, the National Cybersecurity Policy and Strategy, sectoral cybersecurity guidelines issued by regulators such as the Central Bank of Nigeria, and the National Artificial Intelligence Strategy.[4] These instruments provide useful building blocks, but they were not all designed specifically for AI. As a result, they do not yet provide a comprehensive legal architecture for algorithmic accountability, AI safety, model governance, high-risk AI classification, public-sector AI procurement, AI audit, or AI-specific cybersecurity obligations.

This article evaluates Nigeria's legal and regulatory framework for AI governance and cybersecurity. It makes three central arguments. First, Nigeria's strongest existing AI governance foundation is data protection law, particularly because AI systems depend on personal data and automated processing. Secondly, Nigeria's cybersecurity framework provides important protection against cybercrime, critical information infrastructure attacks and cyber incidents, but it does not yet adequately address AI-specific cyber threats. Thirdly, Nigeria requires a coherent risk-based AI governance framework that integrates privacy, cybersecurity, consumer protection, human rights, sectoral regulation and innovation policy.

II. Conceptualising AI Governance and Cybersecurity

AI governance refers to the legal, institutional, ethical and technical mechanisms used to guide the design, development, deployment, monitoring and use of AI systems. It includes rules on data quality, transparency, fairness, accountability, safety, human oversight, explainability, documentation, audit, risk management and redress.[5] AI governance is broader than data protection because AI harms can arise even where no personal data is processed. For example, an AI system may produce unsafe medical advice, generate defamatory content, distort market behaviour, misclassify businesses, facilitate cyber fraud, or support harmful public decisions without necessarily violating privacy law. Proper AI governance must therefore address both individual rights and systemic risks.

Cybersecurity, by contrast, concerns the protection of computer systems, networks, data, infrastructure and digital services against unauthorised access, misuse, disruption, alteration, destruction and exploitation.[6] When AI is introduced into cybersecurity analysis, the relationship becomes complex. AI systems can be targets of cyberattacks, tools used by attackers, or defensive instruments deployed by organisations and governments. This creates three regulatory questions. First, how should the law protect AI systems from cyber compromise? Secondly, how should the law prevent malicious use of AI for cybercrime? Thirdly, how should the law regulate AI-enabled cybersecurity tools, particularly where such tools monitor individuals, inspect communications, profile users, or make automated decisions?

The intersection between AI governance and cybersecurity is especially important in Nigeria because many AI applications depend on personal data, financial data, biometric data and communications infrastructure. If a financial institution uses machine-learning models for fraud detection, the model must be

[3]National Centre for Artificial Intelligence and Robotics and National Information Technology Development Agency, *National Artificial Intelligence Strategy*<https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf> accessed 24 June 2026.

[4] Nigeria Data Protection Act 2023 <https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf> accessed 28 June 2026; Cybercrimes (Prohibition, Prevention, etc.) Act 2015; Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024

[5]European Parliament and Council, *Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence*<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> accessed 26 June 2026.

[6]Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 1.

accurate, secure, auditable and fair. If a government agency deploys biometric identification or predictive analytics, it must comply with constitutional privacy protections, data protection principles and cybersecurity safeguards. If a platform uses AI to moderate content, recommend political information or detect harmful posts, the system may affect freedom of expression, democratic participation and public order.[7] Therefore, AI governance must be treated not simply as technology policy but as a rule-of-law issue.

III. Constitutional and Human Rights Foundations

The Nigerian Constitution provides the first foundation for AI governance through its protection of privacy. Section 37 of the Constitution guarantees the privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications.[8] Although the language of section 37 predates modern AI and digital platforms, its underlying value is highly relevant to automated data processing, digital surveillance, biometric identification, profiling, online tracking and AI-enabled monitoring. AI systems that collect, infer or process personal information may therefore implicate constitutional privacy rights.

The constitutional framework is also relevant because AI may affect equality, dignity, fair hearing, freedom of expression, property rights and access to justice. For instance, algorithmic decision-making may disadvantage individuals on the basis of gender, ethnicity, disability, religion, location, age or socio-economic status if the training data reflects historical bias or if the model is poorly designed. Automated public-sector decisions may also raise fair hearing concerns where affected persons are denied reasons, human review or a meaningful opportunity to challenge the outcome.[9] In this sense, AI governance in Nigeria must be rights-based, not merely innovation-driven.

A rights-based approach does not mean that AI should be discouraged. Rather, it means that innovation must be aligned with constitutional values. The Nigerian state has a legitimate interest in promoting digital development, but it must also ensure that AI does not become a tool for arbitrary surveillance, opaque exclusion, discriminatory service delivery or cyber-enabled exploitation. The Constitution should therefore guide the interpretation of statutory and regulatory instruments dealing with AI, cybersecurity, data protection and digital platforms.

IV. The Nigeria Data Protection Act 2023 as an AI Governance Instrument

The Nigeria Data Protection Act 2023 is the most important existing statute for AI governance in Nigeria. Its importance lies in the fact that many AI systems depend on personal data, whether for training, testing, deployment, profiling or automated decision-making. The Act applies to the processing of personal data by automated and non-automated means where the controller or processor is domiciled, resident or operating in Nigeria, where processing occurs in Nigeria, or where a foreign controller or processor processes personal data of data subjects in Nigeria.[10] This gives the Act extraterritorial relevance and makes it applicable to foreign AI service providers that process personal data of persons in Nigeria.

The Act establishes the Nigeria Data Protection Commission and gives it functions that are directly relevant to AI. These include regulating technological and organisational measures for personal data protection, fostering personal data protection technologies, registering data controllers and processors of major importance, receiving complaints, collaborating with relevant bodies, advising government on policy, regulating cross-border transfers and issuing regulations, directives, codes and guidelines.[11] These powers can be used to shape AI governance even before Nigeria enacts a dedicated AI statute.

The Act sets out core principles of personal data processing, including lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, security, confidentiality, integrity, availability and accountability.[12] These principles map closely onto AI governance concerns. Data minimisation challenges indiscriminate scraping and excessive collection of personal data for AI training. Purpose limitation restricts the repurposing of data for AI uses that are incompatible with the original purpose of collection. Accuracy is crucial where AI systems generate decisions about individuals. Security and

[7]National Information Technology Development Agency, *Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries*<https://nitda.gov.ng/wp-content/uploads/2022/06/Code-of-Practice.pdf>accessed 26 June 2026.

[8]Constitution of the Federal Republic of Nigeria 1999 (as altered), s 37.

[9]Constitution of the Federal Republic of Nigeria 1999 (as altered), ss 36, 37, 39 and 42.

[10]Nigeria Data Protection Act 2023, s 2, <https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf> accessed 26 June 2026.

[11]Nigeria Data Protection Act 2023, ss 4–6.

[12]Nigeria Data Protection Act 2023, s 24.

confidentiality require controllers and processors to protect the data pipelines on which AI systems depend. Accountability requires organisations to demonstrate compliance rather than merely claim it.

The Act also requires lawful bases for processing personal data, including consent, contractual necessity, legal obligation, vital interests, public interest or official authority, and legitimate interests subject to the rights and freedoms of the data subject.[13] In the AI context, this is significant because organisations cannot simply rely on technological capability as a justification for processing personal data. They must identify a lawful basis. This is particularly important for AI training datasets, biometric systems, targeted advertising, credit scoring, workplace monitoring, health analytics and automated public-service decisions.

Another important feature is the requirement for data privacy impact assessments where processing is likely to result in high risk to the rights and freedoms of data subjects.[14] AI systems that involve profiling, biometric identification, large-scale surveillance, automated decision-making, sensitive data or vulnerable groups should ordinarily trigger impact assessment obligations. A properly designed impact assessment should examine necessity, proportionality, risks, safeguards and security measures. However, the Nigerian framework would benefit from developing a specific AI impact assessment template that extends beyond privacy to include discrimination, explainability, safety, cybersecurity, environmental impact, labour impact and public accountability.

The Act also recognises rights relating to automated decision-making. A data subject has the right not to be subject to a decision based solely on automated processing, including profiling, where the decision produces legal or similarly significant effects. Where exceptions apply, the controller must implement safeguards, including the right to obtain human intervention, express a point of view and contest the decision.[15] This is a major AI governance provision. It means that AI-based credit denial, employment screening, insurance decisions, welfare decisions, school admissions, health triage and similar automated outcomes may require human review and contestability where they significantly affect individuals.

The limitation, however, is that the Act addresses automated decisions only through the lens of personal data. It does not create a general AI accountability regime for non-personal-data systems, generative AI, recommender systems, public-sector risk assessment tools, autonomous systems or AI models embedded in infrastructure. It also does not provide a comprehensive classification of high-risk AI systems, mandatory algorithmic audits, conformity assessments, public AI registers, model cards, training-data documentation or post-market monitoring. The Data Protection Act is therefore necessary but not sufficient.

The Act's data security provisions are also significant. Controllers and processors must implement appropriate technical and organisational measures to ensure security, integrity and confidentiality of personal data, including protection against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure or access.[16] Measures may include pseudonymisation, encryption, resilience of systems, restoration processes, risk assessments, testing and regular updating of safeguards.[17] These obligations are directly relevant to AI because AI systems can leak data, reproduce memorised personal information, expose training data, or be compromised through model and data attacks. Nevertheless, Nigerian law should go further by specifying AI security controls such as adversarial testing, model access controls, prompt injection safeguards, secure model deployment, dataset provenance, red-team testing and logging of AI outputs.

The Act further requires personal data breach notification to the Commission within 72 hours where the breach is likely to result in risks to rights and freedoms.[18] This is important for cybersecurity governance. However, AI-specific incident reporting should be broader than personal data breaches. It should include model compromise, harmful autonomous behaviour, significant bias incidents, deepfake fraud, security vulnerability exploitation and material failures of high-risk AI systems.

V. The Cybercrimes Act and the Cybersecurity Framework

Nigeria's principal cybersecurity statute is the Cybercrimes (Prohibition, Prevention, etc.) Act 2015, amended in 2024. The Act seeks to provide a legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes, as well as the protection of critical national information infrastructure, computer systems, networks, electronic communications, data, computer programs, intellectual property and privacy rights.[19] It criminalises a wide range of cyber activities, including unlawful

[13]Nigeria Data Protection Act 2023, s 25.
[14]Nigeria Data Protection Act 2023, s 28.
[15]Nigeria Data Protection Act 2023, s 37.
[16]Nigeria Data Protection Act 2023, s 39(1).
[17]Nigeria Data Protection Act 2023, s 39(2).
[18]Nigeria Data Protection Act 2023, s 40.
[19]Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 1; Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024,

access, system interference, unlawful interception, computer-related forgery, computer-related fraud, identity theft, phishing, spamming, malware-related conduct and attacks on critical infrastructure.[20]

The Act is important for AI governance because AI can be used to facilitate cybercrime. Generative AI can produce phishing messages, fake identities, malware code, synthetic voice fraud, deepfake videos and automated social engineering. AI systems can also be attacked through unauthorised access, data manipulation, model theft, system interference or compromise of cloud infrastructure. Existing cybercrime offences may therefore apply to many AI-enabled cyber harms. For example, unauthorised access to a machine-learning system, manipulation of training data, theft of model weights, or deployment of AI tools for fraud may be prosecuted under existing cybercrime provisions where the statutory elements are met.

The Act also provides for the designation and protection of critical national information infrastructure.[21] This is relevant because AI systems may increasingly be integrated into critical sectors such as banking, telecommunications, energy, transportation, public identity, health, elections and security. If AI becomes embedded in critical infrastructure, then attacks on AI systems may produce national security, public safety or economic consequences. Nigeria should therefore ensure that critical information infrastructure protection expressly covers AI systems, AI-enabled control systems, model repositories, high-risk datasets and cloud infrastructure supporting essential services.

Institutionally, the Act assigns a coordinating role to the Office of the National Security Adviser. The ONSA is responsible for coordinating relevant security and enforcement agencies, supporting cybercrime prevention, ensuring the formulation and implementation of national cybersecurity strategy and policy, establishing and maintaining a national Computer Emergency Response Team Coordination Centre, establishing a national computer forensic laboratory, building capacity, promoting public-private partnerships and coordinating international cybersecurity cooperation.[22] This creates an important national cybersecurity architecture. However, AI governance requires additional coordination with the Nigeria Data Protection Commission, NITDA, sector regulators, law enforcement agencies, consumer protection authorities and human rights institutions.

The 2024 amendment strengthens some aspects of the cybercrime regime. It revises cyber threat reporting requirements by moving from a seven-day reporting window to a 72-hour period from detection for relevant incidents.[23] It also aligns records retention and protection of data with the Nigeria Data Protection Act and introduces stronger sectoral cyber incident structures by requiring sectoral computer emergency response teams or security operation centres in certain contexts.[24] These developments are positive because they move Nigerian cybersecurity governance toward faster incident response and closer integration with data protection.

However, the Cybercrimes Act remains primarily a cybercrime and cybersecurity statute. It is not an AI governance statute. It does not impose AI lifecycle duties, distinguish between low-risk and high-risk AI, require algorithmic transparency, regulate generative AI, establish AI audit duties, or create safeguards against discriminatory automated decisions. It also needs careful rights-sensitive implementation. Cybersecurity regulation must not become a justification for disproportionate surveillance, excessive restrictions on expression, or arbitrary access to communications. The legitimacy of AI-related cybersecurity enforcement will depend on legality, necessity, proportionality, judicial oversight and accountability.

VI. NITDA, Digital Regulation and the National AI Strategy

The National Information Technology Development Agency Act 2007 established NITDA as a central institution for information technology development and regulation in Nigeria. NITDA's mandate includes planning, research, development, standardisation, application, coordination, monitoring, evaluation and regulation of information technology practices.[25] Although the Act predates modern AI, NITDA has become a key actor in Nigeria's emerging AI governance landscape. Its role is visible in digital economy regulation, data protection history, platform governance, emerging technology policy and the development of AI strategy through the National Centre for Artificial Intelligence and Robotics.

<https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2024.pdf> accessed 26 June 2026.

[20]Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss 5–36.

[21]Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss 3–4.

[22]Cybercrimes (Prohibition, Prevention, etc.) Act 2015, s 41.

[23]Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, amendment to s 21, available at <https://cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2024.pdf> accessed 28 June 2026.

[24]Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024, amendments to ss 38 and 41.

[25]National Information Technology Development Agency Act 2007, s 6.

The National Artificial Intelligence Strategy is Nigeria's clearest policy statement on AI. It recognises AI as a strategic technology and seeks to guide responsible adoption, local innovation, ethical development, inclusion and sustainable development.[26] The strategy identifies pillars relating to infrastructure, ecosystem development, sectoral transformation, responsible and ethical AI, and robust AI governance.[27] It also contemplates national AI principles, an AI governance regulatory system, transparent guidelines, risk management frameworks and an AI governance regulatory body.[28]

The strategy is a major policy advancement because it recognises that AI cannot be governed only through scattered rules. It correctly identifies the need for trust, transparency, accountability, risk management and alignment with international best practices. It also acknowledges cybersecurity, data integrity, privacy, legal and regulatory risks as part of the AI risk environment.[29] In this respect, Nigeria is moving in the right direction.

The weakness, however, is that strategy is not the same as enforceable law. Unless its principles are translated into binding obligations, institutional mandates, regulatory standards and enforcement mechanisms, AI governance may remain aspirational. Nigeria therefore needs to decide whether AI regulation will be handled through a new AI Act, amendments to existing laws, sector-specific regulatory instruments, or a hybrid approach. A hybrid model may be most practical: a national AI governance statute or framework law should set general principles, risk classifications and institutional coordination mechanisms, while sector regulators issue detailed rules for finance, health, education, telecommunications, public administration, security and consumer markets.

NITDA's Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries is also relevant. The Code seeks to promote online safety, combat harmful content, address misinformation and disinformation, and create a safer digital ecosystem through a co-regulatory approach.[30] Although it is not an AI statute, it matters because AI-driven recommender systems, content moderation tools, bots and generative AI content are central to platform governance. Nigeria's platform rules should therefore be updated to address AI-generated misinformation, deepfakes, synthetic media labelling, bot disclosure, algorithmic amplification, political advertising transparency and appeal mechanisms for automated content moderation.

VII. Sectoral Cybersecurity and Financial Technology Regulation

Nigeria's financial sector is one of the most AI-relevant sectors because banks, payment service providers and fintech companies use automated fraud detection, credit scoring, transaction monitoring, customer verification, anti-money laundering tools and cybersecurity analytics. The Central Bank of Nigeria has issued risk-based cybersecurity frameworks and guidelines for banks and payment service providers. These frameworks require regulated institutions to adopt cybersecurity governance, risk management, resilience, reporting and testing measures.[31] In the AI context, financial institutions should integrate AI model governance into cybersecurity and operational risk management. This includes validating models, monitoring drift, preventing discriminatory credit outcomes, protecting customer data, testing AI-based fraud systems and ensuring human oversight for significant automated decisions.

Other sector regulators also matter. The Nigerian Communications Commission regulates telecommunications infrastructure and service providers, which are essential to AI deployment and

[26]National Centre for Artificial Intelligence and Robotics and National Information Technology Development Agency, *National Artificial Intelligence Strategy*<https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf> accessed 28 June 2026.

[27]National Centre for Artificial Intelligence and Robotics and National Information Technology Development Agency, *National Artificial Intelligence Strategy*<https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf> accessed 28 June 2026.

[28]National Centre for Artificial Intelligence and Robotics and National Information Technology Development Agency, *National Artificial Intelligence Strategy*, Pillar 5 <https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf> accessed 28 June 2026.

[29]National Centre for Artificial Intelligence and Robotics and National Information Technology Development Agency, *National Artificial Intelligence Strategy*, section on AI risks and mitigation strategies <https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf> accessed 28 June 2026.

[30]National Information Technology Development Agency, *Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries*<https://nitda.gov.ng/wp-content/uploads/2022/06/Code-of-Practice.pdf>accessed 28 June 2026.

[31]Central Bank of Nigeria, *Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers*<https://usercontent.one/wp/www.acaebin.org/wp-content/uploads/2023/07/RISK20BASED20CYBERSECURITY20FRAMEWORK20FINAL201.pdf.pdf>accessed 28 June 2026

cybersecurity. Health regulators will be relevant for AI diagnostics and clinical decision-support tools. The Securities and Exchange Commission will be relevant for algorithmic trading, robo-advisory services and tokenised digital markets. The Federal Competition and Consumer Protection Commission will be relevant where AI systems mislead consumers, enable unfair contract terms, facilitate price manipulation or create deceptive outputs.[32] This sectoral reality confirms that AI governance cannot be assigned to a single institution without coordination. Nigeria needs a whole-of-government framework.

VIII. Strengths of Nigeria's Current Framework

Nigeria's framework has several strengths. First, the Data Protection Act provides a modern baseline for privacy, data security and automated decision-making. This is important because data is the foundation of most AI systems. The Act's principles of fairness, transparency, data minimisation, security and accountability can constrain irresponsible AI practices.[33] The recognition of rights relating to automated decisions is particularly important because it gives individuals a legal basis to challenge certain forms of algorithmic decision-making.[34]

Secondly, the Cybercrimes Act provides a legal framework for prosecuting cybercrime and protecting critical information infrastructure. It establishes institutional structures for cyber incident response and national coordination. This is important in an AI environment because malicious actors can use AI to scale cyberattacks, while attackers may also target AI systems themselves.[35]

Thirdly, the National AI Strategy shows that Nigeria recognises AI as a national development priority and is aware of governance risks. The strategy's emphasis on ethical AI, governance principles, risk management and regulatory coordination provides a policy foundation for future law reform.[36]

Fourthly, Nigeria's sectoral regulators have begun to address cybersecurity in high-risk sectors such as banking and payments. This is valuable because AI risks vary by sector. A general AI framework should therefore be complemented by sector-specific rules.

Fifthly, Nigeria has an innovation policy foundation through instruments such as the Nigeria Startup Act 2022, which seeks to support digital innovation, entrepreneurship and startup ecosystems.[37] This matters because AI governance should not only restrict risk; it should also enable responsible local innovation. Nigeria must avoid a regulatory model that is so burdensome that only large foreign technology companies can comply, while local startups are excluded.

IX. Gaps and Weaknesses

Despite these strengths, Nigeria's framework has significant gaps. The most important gap is the absence of a comprehensive AI law. Existing laws regulate fragments of AI: data protection regulates personal data processing; cybercrime law regulates cyber offences and infrastructure protection; sectoral rules regulate specific industries; platform codes regulate online intermediaries. None of these instruments provides a complete AI lifecycle governance regime. There is no binding national classification of prohibited, high-risk, limited-risk and low-risk AI systems. There are no general duties on AI developers to document training data, test models, assess bias, disclose limitations, conduct conformity assessments or monitor post-deployment harms.

A second weakness is institutional fragmentation. AI governance touches NITDA, the Nigeria Data Protection Commission, the Office of the National Security Adviser, the Central Bank of Nigeria, the Nigerian Communications Commission, law enforcement agencies, consumer protection authorities and sector regulators. Without clear coordination, overlapping mandates may create regulatory uncertainty. Organisations may face inconsistent requirements, while harmful AI deployments may fall between regulatory gaps. Nigeria needs formal coordination mechanisms, joint guidance, memoranda of understanding, shared reporting channels and a lead AI governance body with clearly defined powers.

A third weakness is the limited specificity of cybersecurity obligations for AI systems. General cybersecurity duties are useful but insufficient. AI systems have distinctive vulnerabilities. Training data can be

[32]Federal Competition and Consumer Protection Act 2018, <https://fccpc.gov.ng/wp-content/uploads/2022/07/FCCPA-2018.pdf> accessed 28 June 2026.
[33]Nigeria Data Protection Act 2023, s 24.
[34]Nigeria Data Protection Act 2023, s 37.
[35]Cybercrimes (Prohibition, Prevention, etc.) Act 2015, ss 1, 3, 5–36 and 41.
[36]National Centre for Artificial Intelligence and Robotics and National Information Technology Development Agency, *National Artificial Intelligence Strategy*, Pillar 5 <https://ncair.nitda.gov.ng/wp-content/uploads/2025/09/National-Artificial-Intelligence-Strategy-19092025.pdf> accessed 28 June 2026.
[37]Nigeria Startup Act 2022, <https://startup.gov.ng/> accessed 28 June 2026.

poisoned. Models can be extracted. Prompts can be manipulated. Outputs can reveal sensitive information. Generative systems can be used to create convincing fraud. Autonomous systems can behave unpredictably when exposed to hostile inputs. Nigerian law should therefore require AI-specific security controls for high-risk systems, including secure development, dataset provenance, adversarial testing, access control, logging, human override, incident reporting and independent audit.

A fourth weakness concerns algorithmic transparency and explainability. The Data Protection Act provides transparency rights in relation to personal data and automated decisions, but Nigeria lacks broader transparency obligations for AI systems that affect the public. Citizens should know when they are interacting with AI in significant contexts. Public bodies should disclose high-risk AI systems used in decision-making. Organisations deploying AI in employment, credit, insurance, education, health care and policing should provide meaningful information about the logic, consequences, limitations and review mechanisms of such systems.

A fifth weakness is the lack of a public-sector AI procurement framework. Government adoption of AI can improve efficiency, but it can also produce serious rights risks. Public agencies may procure AI systems from vendors without adequate testing, documentation, local validation or accountability. Nigeria should require public-sector algorithmic impact assessments before deploying AI systems that affect rights, benefits, enforcement, security or access to public services.

A sixth weakness is enforcement capacity. AI governance requires technical expertise. Regulators need data scientists, cybersecurity specialists, AI auditors, forensic experts, lawyers, ethicists and sector experts. Without adequate capacity, even good laws may remain ineffective. Nigeria must invest in regulator capacity, judicial training, law enforcement expertise, forensic laboratories and public awareness.

A seventh weakness is cross-border dependence. Many AI systems used in Nigeria are developed, hosted or controlled outside Nigeria. Data may be transferred across borders, processed on foreign cloud infrastructure, or governed by foreign contractual terms. The Data Protection Act addresses cross-border personal data transfers, but Nigeria also needs broader digital sovereignty and interoperability strategies. This does not necessarily mean data localisation in every case. Rather, it means Nigeria must ensure that foreign AI providers operating in Nigeria comply with Nigerian law, cooperate with regulators, preserve evidence, protect users and provide accessible redress.

X. Comparative Lessons from International and Regional Developments

Nigeria can draw lessons from international and regional AI governance instruments. The European Union AI Act adopts a risk-based approach, distinguishing between unacceptable-risk AI, high-risk AI, transparency-risk systems and lower-risk applications.[38] High-risk AI systems are subject to obligations relating to risk management, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness and cybersecurity. Nigeria need not copy the EU model wholesale, but it can adopt the principle that regulation should be proportionate to risk.

The OECD AI Principles emphasise inclusive growth, human-centred values, transparency, robustness, safety, security and accountability.[39] The UNESCO Recommendation on the Ethics of Artificial Intelligence stresses human rights, dignity, fairness, transparency, human oversight and social responsibility.[40] The African Union Continental AI Strategy provides an Africa-centred policy framework that emphasises ethics, inclusion, human rights, development, capacity and African priorities.[41] These instruments suggest that Nigeria should build an AI governance model that is globally interoperable but locally grounded.

Nigeria's framework should therefore avoid two extremes. It should not be so weak that individuals and businesses are exposed to unaccountable AI harms. It should also not be so rigid that innovation is stifled. The best approach is risk-based, rights-based and innovation-sensitive. Low-risk AI should face light-touch obligations. High-risk AI should face strong obligations. Unacceptable uses, such as AI systems designed for unlawful surveillance, exploitative manipulation or criminal cyber activity, should be prohibited or strictly controlled.

---

[38]European Parliament and Council, *Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence*<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> accessed 28 June 2026.

[39]Organisation for Economic Co-operation and Development, *OECD AI Principles*<https://www.oecd.org/en/topics/sub-issues/ai-principles.html> accessed 28 June 2026.

[40]United Nations Educational, Scientific and Cultural Organization, *Recommendation on the Ethics of Artificial Intelligence*<https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence>accessed 28 June 2026.

[41]African Union, *Continental Artificial Intelligence Strategy*<https://au.int/sites/default/files/documents/44004-doc-EN-_Continental_AI_Strategy_July_2024.pdf> accessed 28 June 2026.

XI. Recommendations for Reform

Nigeria should enact a dedicated AI Governance Act or adopt a binding AI governance framework under a clear statutory mandate. The law should define AI systems broadly enough to cover machine learning, generative AI, automated decision systems and other advanced algorithmic systems. It should classify AI systems by risk. Prohibited AI practices should include systems designed for unlawful biometric surveillance, exploitative manipulation, discriminatory social scoring, criminal cyber automation and other uses inconsistent with constitutional rights. High-risk AI should include systems used in employment, education, credit, insurance, health care, law enforcement, migration, biometric identification, critical infrastructure, public benefits and essential services.

Nigeria should impose lifecycle obligations on developers and deployers of high-risk AI. These should include risk assessment, data governance, cybersecurity-by-design, human oversight, technical documentation, audit logs, transparency notices, accuracy testing, bias assessment, post-deployment monitoring and incident reporting. For generative AI, obligations should include content provenance, synthetic media labelling, safeguards against unlawful content generation, cybersecurity controls and mechanisms to prevent the disclosure of sensitive data.

Nigeria should strengthen the relationship between AI governance and data protection. The Nigeria Data Protection Commission should issue specific guidance on AI and personal data. Such guidance should address lawful bases for AI training, consent limitations, legitimate interests assessments, children's data, biometric data, automated decision-making, data protection impact assessments, generative AI, web scraping, cross-border AI processing and breach notification. Data privacy impact assessments should be expanded into algorithmic impact assessments for high-risk AI.

Nigeria should also develop an AI cybersecurity standard. This standard should require secure model development, secure data pipelines, adversarial testing, prompt injection controls, model access management, protection against model extraction, red-team testing, logging, vulnerability disclosure, incident response and supply-chain security. High-risk AI operators should notify the relevant regulator of serious AI incidents, including cyber compromise, unlawful data exposure, systemic bias, harmful autonomous behaviour and deepfake-enabled fraud affecting users in Nigeria.

Institutional coordination must be improved. A National AI Governance Council or independent AI Governance Commission should include representation from NITDA, NDPC, ONSA, CBN, NCC, FCCPC, sector regulators, academia, civil society, industry and human rights institutions. The body should not duplicate every sector regulator. Instead, it should issue cross-sector standards, maintain a national AI risk register, coordinate enforcement, accredit AI auditors, support regulatory sandboxes and advise government on AI policy.

Public-sector AI requires special rules. Before deploying AI systems that affect rights, benefits, enforcement or access to public services, government agencies should conduct algorithmic impact assessments, publish summaries, provide human review, preserve audit trails and ensure accessible complaint mechanisms. Procurement contracts should require vendors to disclose system limitations, training data provenance, cybersecurity controls, bias testing and audit cooperation.

Nigeria should encourage responsible innovation through sandboxes, standards and capacity building. AI startups should have access to regulatory guidance, testing environments, public datasets, research support and affordable compliance tools. Universities should be supported to develop AI law, cybersecurity, ethics and data science programmes. Judges, regulators, prosecutors and law enforcement officers need training on AI evidence, cybercrime, digital rights and algorithmic accountability.

Finally, Nigeria should cooperate internationally and regionally. AI and cyber threats are cross-border. Nigeria should align with African Union initiatives, participate in international AI standards development, strengthen mutual legal assistance for cybercrime, and require foreign AI providers serving Nigerian users to comply with Nigerian law. A globally interoperable framework will support trade, trust and investment.

XII. Conclusion

Nigeria has made meaningful progress in building the foundations for AI governance and cybersecurity. The Constitution protects privacy and other fundamental rights. The Nigeria Data Protection Act provides strong principles for lawful, fair, secure and accountable processing of personal data. The Cybercrimes Act creates a framework for cybercrime prevention, prosecution, critical information infrastructure protection and national cyber coordination. NITDA and sector regulators have issued important digital and cybersecurity instruments. The National Artificial Intelligence Strategy shows that Nigeria recognises the need for ethical, inclusive and well-governed AI.

However, these instruments remain fragmented. They do not yet amount to a comprehensive AI governance regime. Nigeria's challenge is to move from policy aspiration to enforceable governance. This requires a risk-based AI law or binding framework, AI-specific cybersecurity standards, institutional

coordination, public-sector safeguards, algorithmic transparency, human oversight, auditability and effective remedies. AI can support Nigeria's development, but only if it is governed in a manner that protects rights, strengthens cybersecurity, builds public trust and supports responsible innovation. The future of AI in Nigeria should not be left to market forces, foreign platforms or fragmented regulation. It should be shaped by law, constitutional values, technical competence and democratic accountability.