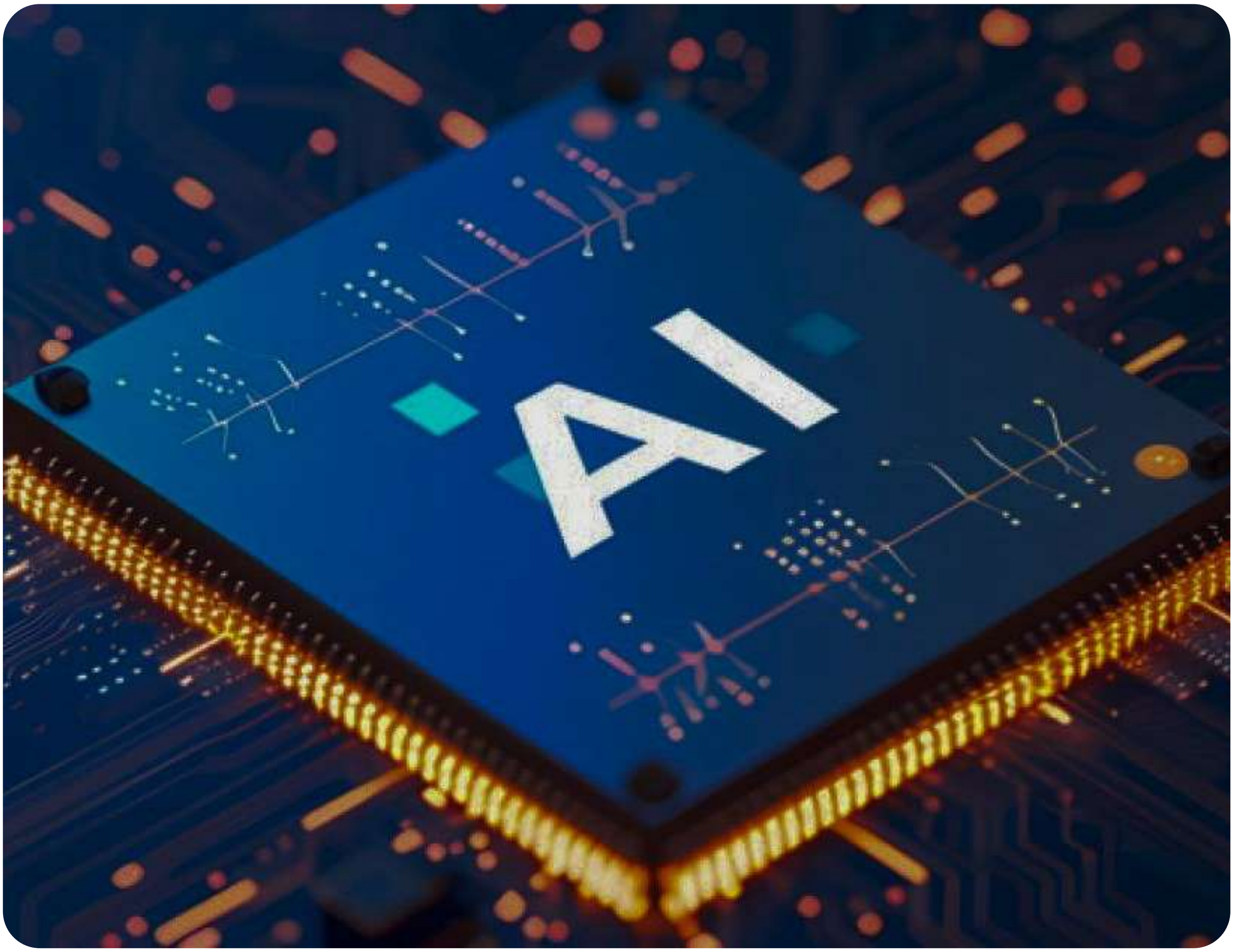
CANDELP

COMMERCIAL & ENERGY LAW PRACTICE

AI UNDER THE NIGERIAN DATA PROTECTION ACT 2023: NAVIGATING NIGERIA'S EMERGING DATA PRIVACY LANDSCAPE

Temitope Omojugba

INTRODUCTION



Artificial Intelligence (AI) is redefining global business and governance. From facial recognition systems and chatbots to automated loan approval engines and predictive policing tools, AI is transforming how we process information and make decisions. In Nigeria, the growing adoption of AI in fintech[1], telecommunications, surveillance, and e-commerce underscore its increasing relevance.

AI can be described as computer systems or technologies that mimic human intelligence to perform tasks such as learning, reasoning, and problem-solving. These systems often require enormous volumes of personal data to function effectively, this data is collected, stored, and analysed in real time.[2]

This poses a significant regulatory question: Can AI systems operating in Nigeria truly comply with the Nigerian Data Protection Act (NDPA) 2023? As AI continues to spread across sectors, so does the need for clear compliance guidance, ethical boundaries, and proactive regulation. This article explores how Nigeria's data privacy framework aligns with emerging AI use cases and whether it is adequately prepared to meet the challenge.

BACKGROUND: HOW NIGERIA GOT HERE

Before the passage of the 2023 NDPA, the country's data protection landscape was governed by the 2019 Nigeria Data Protection Regulation (NDPR), issued by the National Information Technology Development Agency (NITDA). The NDPR marked a critical first step in recognising data protection as a legal issue in Nigeria. However, it lacked statutory force[3], a robust enforcement structure, and sector-specific clarity, especially in rapidly evolving areas such as artificial intelligence, biometrics, and automated decision-making.[4]

As digital services expanded and AI adoption surged across sectors like fintech, health tech, and telecommunications, these limitations became more glaring. Key concerns emerged over unchecked data harvesting, opaque algorithmic profiling, and the absence of clear rules for cross-border data transfers.[5] The NDPR's reliance on interpretive compliance, which meant rules were broadly framed and left for organisations to interpret and apply in their own way, left many businesses without consistent guidance and exposed data subjects to potential abuse.[6]

In response, the Nigerian legislature enacted the NDPA 2023. The Act establishes the Nigeria Data Protection Commission (NDPC)[7] as an independent regulatory body and grants it express powers to investigate breaches, conduct audits, issue compliance directives, and impose sanctions. It codifies essential data protection principles: lawfulness, fairness, transparency, purpose limitation, and accountability, and aligns with global standards such as the EU General Data Protection Regulation (GDPR).[8]

More importantly, the NDPA introduces a forward-looking, rights-based approach designed to accommodate emerging technologies. It addresses specific risks associated with AI, such as automated decision-making without human oversight, the use of sensitive personal data in predictive systems, and the need for transparency in algorithmic outcomes. With this shift, the NDPA serves as Nigeria's foundational compliance framework, particularly for data-intensive and AI-driven industries.[9]

OVERVIEW OF THE NDPA 2023: CORE PRINCIPLES

The 2023 NDPA establishes clear responsibilities for data controllers and processors. These responsibilities have direct implications for developers and operators of Artificial Intelligence (AI) systems. The core obligations are primarily outlined in Sections 24 to 39 of the Act[10] and are further interpreted through the General Application and Implementation Directive (GAID).

The following principles are central to the NDPA's data protection framework:

- **Lawfulness, Fairness, and Transparency Section 24(1)(a):** AI systems must process personal data lawfully and fairly, with a valid legal basis and transparent communication to the data subjects.

- **Purpose Limitation Section 24(1)(b):** Data must be collected for specific, clear, and legitimate purposes and must not be used in ways that are incompatible with those purposes.

- **Data Minimisation Section 24(1)(c):** Only the minimum amount of data necessary to achieve the intended purpose should be collected and processed.

- **Accuracy and Storage Limitation Sections 24(1)(e) and (f):** Personal data must be accurate and kept up to date. It must not be retained for longer than necessary to fulfil the original purpose for which it was collected.

- **Security, Confidentiality, and Integrity Section 24(1)(f); GAID Article 15(1)(6):** Data must be protected using appropriate technical and organisational measures that ensure its confidentiality, integrity, and availability.

- **Rights of Data Subjects (Sections 34 to 36):** Individuals have the right to access their data, request corrections, demand erasure, object to processing, and exercise control over how their data is used.

- **Automated Decision Making (Section 37):** Individuals must not be subject to decisions that produce legal or significant effects solely based on automated processing unless there are appropriate safeguards and a right to human review.

- **Data Protection Impact Assessments (DPIAs) (Section 28):** Where data processing presents a high risk to individuals' rights and freedoms, such as in large-scale AI applications, a DPIA must be carried out to identify and mitigate potential harms.

The General Application and Implementation Directive (GAID) issued under the 2023 NDPA sets out eight ethical principles that support the interpretation and application of this Act. These principles are especially vital in the context of Artificial Intelligence (AI), where automated decisions can affect individuals in complex, non-transparent, and potentially irreversible ways.

The eight ethical principles are:

- Fairness
- Purpose Limitation
- Data Minimisation
- Ethics
- Storage Limitation
- Data Accuracy
- Confidentiality and Accountability
- Duty of Care[11]

AI AND THE NDPA COLLIDE

AI systems often function in ways that unintentionally challenge the NDPA's core principles. These functions include;

1. **Consent and Lawfulness:** AI tools often reuse personal data for new purposes not originally agreed to by the data subject. For instance, a ride-hailing platform may collect location data to match drivers and riders but later use that same data to profile users or deliver targeted ads. Such reprocessing without fresh consent breaches the requirement that data processing be lawful, fair, and transparent.[12]

2. **Purpose Limitation:** AI systems are built to learn and adapt by identifying patterns in data, often beyond the initial scope of collection. However, the NDPA requires that personal data must be collected for specific, legitimate purposes and not be further processed in a way incompatible with those purposes unless a legal basis exists.[13]

3. **Data Minimisation:** Machine learning models tend to thrive on large volumes of data, increasing accuracy with more inputs. This contradicts the principle of data minimisation, which demands that only the data necessary for the intended purpose be collected and processed.[14]

4. **Transparency:** AI's inner workings, especially deep learning models, are often opaque even to developers. This makes it difficult for data subjects to understand how decisions affecting them are made and to exercise their rights effectively.[15]

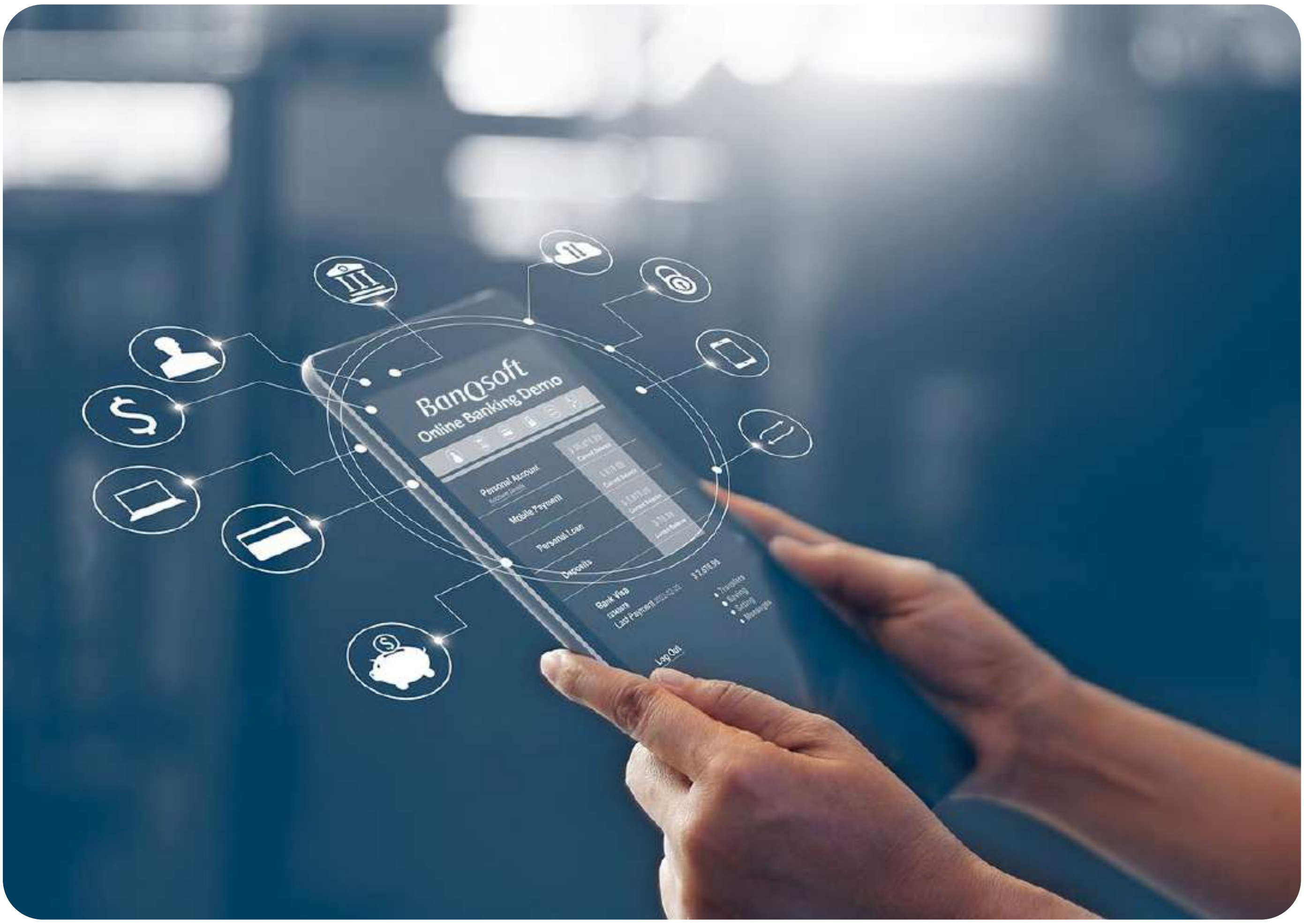
5. **Automated Decision-Making:** When AI systems make decisions such as approving loans or filtering job applications without human involvement, this can violate provisions that require human oversight or informed consent for significant decisions based solely on automated processing.[16]

HYPOTHETICAL EXAMPLE:

Consider a scenario in which a Nigerian digital bank deploys an AI system to automatically reject loan applications from individuals labelled as "high risk" based on their web browsing activity and mobile phone usage patterns. The system does not offer applicants an opportunity to appeal the decision through human review. Such an approach would likely contravene Section 37 of the 1999 Constitution as amended,[17] which guarantees the right to privacy, and would also breach the transparency and accountability principles set out in the NDPA, particularly in relation to automated decision making and fairness.[18]

In Chukwunweike Akosa Araka v. Ecart Internet Services Nigeria Ltd, the applicant had ordered meals via Jumia Food and provided his personal details solely for the purpose of completing the transaction. Seven months later, he began receiving direct marketing messages from Domino Pizza, despite never sharing his contact information directly with the restaurant.

The Lagos State High Court held that using his personal data for unsolicited marketing, when it had been provided exclusively for order fulfilment, breached the purpose limitation principle under the Nigerian Data Protection Act. The court affirmed that such processing was unlawful without the data subject's explicit consent. This decision sets an important precedent for how Nigerian courts may view the unlawful repurposing of data, including by artificial intelligence systems, particularly where consent is narrowly defined and not expressly granted for secondary uses.



HOW TO NAVIGATE COMPLIANCE

To mitigate AI's friction with the NDPA, data controllers and AI developers must embed compliance into the development lifecycle. This can be done in the following ways;

1. Conduct DPIAs

DPIAs are mandatory where AI systems are likely to impact data subjects' rights. Section 29 requires organisations to assess and document risks before deployment.[19]

2. Adopt Privacy by Design and Default

This includes:

- Limiting access to data
- Using synthetic or anonymised datasets
- Designing systems that default to the maximum privacy-protective settings[20]

3. Apply Technical Safeguards

This includes:

- **Federated Learning:** This is a privacy-preserving way of training artificial intelligence models. Instead of collecting and storing all data in one central location, the model is trained directly on each device or server where the data is stored. Only the "lessons learned" (model updates) are shared, not the raw data itself. This means sensitive information never leaves its original location, reducing the risk of breaches and ensuring compliance with data protection laws.
- **Algorithmic Audits:** Regularly check for bias, accuracy, and data integrity[21]

4. Establish Internal Governance

Organisations should maintain:

- AI ethics review boards
- Data governance charters
- Vendor review protocols[22]

5. Contractual Protections

Under GAID Article 34, data controllers must execute Data Processing Agreements (DPAs) with AI vendors. DPAs must define:

- Scope of processing
- Security controls
- Breach reporting obligations
- Rights of audit and oversight[23]

6. Maintain Transparency and Explainability

AI systems, especially those making automated decisions, must be explainable. Under Section 38 of the NDPA, data subjects have a right to meaningful information about the logic involved in automated decision-making[24]. Organisations should therefore:

- Offer clear documentation of how AI models make decisions
- Provide plain-language explanations to data subjects upon request
- Use interpretable models where possible

7. Implement Data Subject Rights Mechanisms

This can be done by ensuring systems and processes are in place to uphold NDPA rights, such as the:

- Right to object to processing (especially profiling and automated decisions)
- Right to erasure (right to be forgotten)
- Right to data portability
- Right to access and correction of personal data[25]

This should include user interfaces or backend workflows for receiving, authenticating, and resolving such requests within the required timeline.

8. Ensure Cross-border Data Transfer Compliance

If AI systems process or store data outside Nigeria, controllers must:

- Follow the provisions of Section 41 and the NDPC's Guidelines for Cross-Border Data Transfer, ensuring transfers only occur to countries with adequate protection or under standard contractual clauses.[26]

9. Train Staff and AI Teams on NDPA

Even the most robust compliance mechanisms will fail without adequate human oversight. Companies should:

- Train developers, product teams, and legal/compliance staff on NDPA principles
- Regularly update training as regulations evolve.[27]

Another important consideration under the 2023 NDPA is how consent is obtained from data subjects. While consent remains a lawful basis for processing, it must be specific, informed, unambiguous, and freely given. This means that blanket consents such as generic popups requiring users to "agree to everything" before proceeding may not, on their own, meet the Act's standard. Where multiple processing purposes exist, consent should be obtained in a granular or layered manner, with clear explanations of each purpose and an accessible privacy notice. The process for withdrawing consent should be as simple as the process for giving it

THE ROLE OF THE NDPC MOVING FORWARD

While the NDPA lays a strong foundation, Nigeria's regulatory framework for Artificial Intelligence (AI) is still evolving. The Nigeria Data Protection Commission (NDPC) may implement the following strategies to proactively shape responsible AI governance:

1. **Issue AI Specific Guidance:** The Commission should develop clear, sector-specific rules for AI applications in areas such as healthcare, finance, education, and employment where data sensitivity is high and risks to rights are significant.
2. **Launch Regulatory Sandboxes:** Borrowing from models in Kenya and the UK, the NDPC could adopt regulatory sandboxes that allow AI solutions to be tested in controlled environments. This approach promotes innovation while maintaining oversight and accountability.
3. **Support Industry Codes of Conduct:**Under Section 62 of the NDPA, the NDPC has the power to approve voluntary industry codes of conduct. This can help foster collaboration among stakeholders in developing enforceable standards for transparency, fairness, and ethical AI deployment.
4. **Continue Strong Enforcement:** The NDPC has shown an increasing readiness to investigate and penalise violations of data protection standards. Continued enforcement, especially where AI systems impact privacy, consent, or data security, will be essential in setting a tone of accountability across sectors.

COMPARATIVE GLIMPSE

1. European Union – GDPR and the Proposed EU AI Act

The General Data Protection Regulation (GDPR), under Article 22, limits decisions that have legal or similarly significant effects on individuals from being made solely by automated means, except where the decision is necessary to enter into or perform a contract, is authorised by Union or Member State law, or is based on the individual's explicit consent.

This safeguard was tested in SCHUFA Holding AG (C 634/21, 7 Dec 2023) where the Court of Justice of the EU ruled that generating a credit score can amount to a "solely automated decision" when that score is relied on heavily, such as in deciding whether or not to approve a loan. In such situations, organisations must have a lawful basis, provide transparency, and offer the right to human review.

The EU is currently considering the adoption of an Artificial Intelligence Act, which is designed around a risk-based model of regulation. In its draft form, the Act classifies AI into tiers: systems deemed to pose an "unacceptable risk" (for example, government social scoring) are to be prohibited and categorised "high-risk" applications, such as recruitment, credit scoring, and law enforcement and would face stringent compliance duties; while lower-risk uses would be subject to lighter transparency rules. Since the legislation is still under negotiation, its final scope and impact remain uncertain, but it signals the EU's intention to set the pace for global AI governance.

2. United Kingdom – ICO Guidance

- The UK Information Commissioner's Office (ICO) has issued detailed guidance to support responsible AI use. Key principles include:
  - Ensuring AI systems are explainable and understandable to users;
  - Designing systems to be auditable, enabling oversight and accountability;
  - Embedding fairness and non-discrimination throughout the AI lifecycle.[28]

In the United Kingdom case of Bridges v South Wales Police (Court of Appeal, 2020), the Court found the police's use of live facial recognition technology unlawful due to an inadequate legal framework and a flawed Data Protection Impact Assessment. This judgment reinforced that AI driven decision making, particularly in sensitive contexts, must operate within a robust legal and procedural framework.

3. Kenya – National AI Strategy (2022)

- Kenya's National Artificial Intelligence Strategy, published in 2022, integrates AI governance with its Data Protection Act 2019.
- Their strategy emphasises:
  - Ethics-based regulation aligned with constitutional rights;
  - Promotion of digital literacy, inclusion, and fair access to AI technologies;
  - The need for AI to support national development goals while safeguarding rights and freedom.[29]

As Nigeria continues to advance digitally, we cannot afford to take a wait-and-see approach when it comes to Artificial Intelligence. While the Nigerian Data Protection Act 2023 is a good starting point, especially in terms of how personal data is processed and protected, it is not enough. AI is infiltrating many aspects of our lives. We must also address questions of fairness, bias, discrimination, accountability, and the broader implications for dignity and human rights.

But can AI ever truly be fair? In reality, AI systems are not self-made; they are the products of human design and human data. Every dataset reflects the world from which it was drawn, with all its imperfections, inequalities, and blind spots. Every line of code carries the assumptions and priorities of its creators. This means that AI does not escape human bias; it often inherits it, and in some cases magnifies it at speed and scale. Achieving fairness therefore is not about expecting AI to be neutral by nature, but about building deliberate safeguards such as using diverse and representative datasets, adopting transparent design processes, and carrying out ongoing testing and correction so that AI serves as a check on bias rather than a multiplier of it.

The reality is that AI is already being used in ways that directly affect people's lives. From health care and job recruitment to digital lending and even law enforcement, we are beginning to see the influence of AI tools in everyday decision making. If left unchecked, these tools may produce harmful or biased outcomes often without transparency about how or why the decision was made. Globally, we have already seen cases where credit scoring systems or facial recognition softwares excluded or misidentified people, especially those from vulnerable groups. In Nigeria, similar risks exist, even if it has not gained widespread attention.

To avoid the confusion and inefficiency that arise from fragmented or overlapping laws, Nigeria needs a coordinated governance framework for AI. When legal responsibilities are split across multiple agencies without alignment, progress slows, innovators face uncertainty, and enforcement weakens. A unified approach under a single, coherent vision will ensure that regulation keeps pace with technological change while maintaining clarity and accountability.

We also need to be clear about who is responsible when something goes wrong. If an AI tool makes a bad decision or causes harm, who should be held accountable? Is it the company that built it, the one that uses it, or the person affected by it? There should also be a simple and fair way for people to challenge decisions made by AI or to get justice when they have been wronged.

Regulation is always a tough space, particularly when balancing innovation with the protection of people's rights. One practical step in achieving this balance is to set up a national task force dedicated to AI, working closely with data protection regulators and other relevant agencies to develop sector-specific guidelines for AI use. Drafting a national policy on AI governance will also be beneficial, as it can provide a unified framework that complements existing laws by filling regulatory gaps, setting clear ethical standards, and offering practical implementation strategies. While laws often outline broad obligations, such a policy can translate these into detailed, context-specific rules that address emerging risks, guide industry practices, and ensure that innovation aligns with Nigeria's socio-economic priorities.

CONCLUSION

Artificial Intelligence is no longer a distant concept; it is already influencing Nigeria's digital economy in profound ways. With its rapid adoption comes the responsibility to govern it carefully and thoughtfully. The NDPA 2023 offers an important legal foundation for managing data-related risks, but on its own, it may not capture the full complexity of AI without additional guidance, sector-specific standards, and effective enforcement.

A central challenge is ensuring that regulation keeps pace with technological change while clearly defining responsibility when AI systems cause harm. Accountability should rest primarily with the entity that deploys and operates the AI, while developers share responsibility for design flaws or inadequate safeguards. International experience provides useful lessons. The European Union, through its AI Act and the proposed AI Liability Directive, establishes a risk-based approach with clear obligations for both developers and deployers of high-risk systems. Canada's proposed Artificial Intelligence and Data Act emphasises accountability, transparency, and accessible remedies. In the United States, regulators such as the Federal Trade Commission have held companies accountable for harmful or discriminatory AI outcomes using existing consumer protection frameworks. These examples demonstrate that Nigeria can adopt a similar approach, ensuring that victims of harmful AI decisions have clear channels for redress.

For this framework to succeed, businesses may embed ethical design, transparency, and compliance into every stage of AI development and deployment. Regulators must coordinate to close legal and technical gaps while ensuring clarity and fairness. Lawyers and legal advisors play a crucial role in translating principles into practical strategies that protect both innovation and the public interest.

Ultimately, the future of AI in Nigeria will be shaped not just by technology, but by deliberate legal, ethical, and governance choices that include clear accountability and avenues for justice. The time to act is now, before innovation moves faster than regulation and preventable harm occurs.

1. Ema Ogbe, Chinelo Obiekwe, Artificial Intelligence and Nigerian Data Protection. https://www.mondaq.com/nigeria/privacy-protection/1505422/artificial-intelligence-and-nigerian-data-protection accessed on the 22nd of July 2025.

2. Black AI by McKinsey, The Data Driven Enterprise of 2025. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-data-driven-enterprise-of-2025 accessed on the 22nd of July 2025.

3. Mercy King'Ori, Nigeria's New Data Protection Act Explained https://fpf.org/blog/nigerias-new-data-protection-act-explained/ accessed on the 22nd of July 2025.

4. KPMG-The Nigeria Data Protection Act 2023 https://assets.kpmg.com/content/dam/kpmg/ng/pdf/the-nigeria-data-protection-act-2023.pdf accessed on the 22nd of July 2025.

5.

6. ICLG-Data Protection Laws and Regulations Nigeria 2025 https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria accessed on the 22nd of July 2025.

7. Nigeria Data Protection Act 2023

8. Harlem Solicitors, Legal Protection of Data in the Nigerian Digital Space https://www.harlemsolicitors.com/2025/05/07/legal-protection-of-data-in-the-nigerian-digital-space/ accessed on the 22nd of July 2025.

9.

10. Sections 24-39 Nigerian Data Protection Act 2023

11. Nigeria Data Protection Commission, General Application and Implementation Directive (GAID), 2023, Section 15 Ethical Principles for Processing Personal Data.

12. Section 24(1)(a) NDPA; GAID Article 18

13. Section 24(1)(b) NDPA; GAID Schedule 1(2)

14. Section 24(1)(c) NDPA

15. Section 24(1)(a) NDPA

16. Section 37 NDPA

17. Section 37 Constitution of the Federal Republic of Nigeria, 1999 (as amended)

18. Sections 24(2)(a), 30, and 38, Nigeria Data Protection Act 2023

19. Nigeria Data Protection Act 2023, Section 29 – Data Protection Impact Assessments https://ndpc.gov.ng/wp-content/uploads/2023/10/Nigeria-Data-Protection-Act-2023.pdf accessed on the 27th of July 2025.

20. GDPR Recital 78– Introduces the concept of "Privacy by Design and Default" https://gdpr.eu/recital-78-privacy-by-design/ accessed on the 27th of July 2025.

21. Abadi, M. et al. (2016). Deep Learning with Differential Privacy. https://arxiv.org/abs/1607.00133 accessed on the 27th of July 2025.

22. OECD (2021). Principles on AI Governance. https://www.oecd.org/going-digital/ai/principles/ , Future of Life Institute. AI Governance Frameworks https://futureoflife.org/ai-governance/ accessed on the 1st of August 2025.

23. Global AI and Data Regulations (GAID) – Article 34: Data Processing Agreements.

24. Nigeria Data Protection Act, 2023, Section 38(1)(b)

25. Nigeria Data Protection Act, 2023, Chapter V, sections 35–39

26. Nigeria Data Protection Act, 2023, Section 41, Nigeria Data Protection Commission, Guidelines for Cross-Border Data Transfer, 2023

27. Nigeria Data Protection Commission, Compliance Monitoring and Enforcement Regulation, 2024, Part IV (Training and Awareness Obligations)

28. UK Information Commissioner's Office (ICO), Explaining decisions made with AI (2020). https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/explaining-decisions-made-with-ai/ accessed on the 2nd of August 2025.

29. Ministry of ICT, Innovation and Youth Affairs (Kenya), National Artificial Intelligence Strategy 2022. https://ict.go.ke/kenya-national-artificial-intelligence-strategy/ accessed on the 2nd of August 2025.

Temitope Omojugba

Associate

temitope@acandelp.com