

Volume 2, Issue 3

Research Article

Date of Submission: 17 June, 2026

Date of Acceptance: 02 July, 2026

Date of Publication: 27 July, 2026

Does the Nigeria Data Protection Act (NDPA) Regulate Artificial Intelligence?

Olayimika Oyebanji*

Managing Partner, BlockLaw Consulting, CLO, Aligned Sovereign Intelligence Institute

*Corresponding Author:

Olayimika Oyebanji, Managing Partner, BlockLaw Consulting, CLO, Aligned Sovereign Intelligence Institute, Nigeria.

Citation: Oyebanji, O. (2026). Does the Nigeria Data Protection Act (NDPA) Regulate Artificial Intelligence?. *Arch Interdiscip Educ*, 2(3), 01-03.

Abstract

The Nigeria Data Protection Act (NDPA) 2023 represents the country's primary legal framework for the processing of personal data. Given that data constitutes the foundational architecture of Artificial Intelligence (AI) systems, this paper examines whether the NDPA effectively regulates AI technologies in the absence of a dedicated AI law in Nigeria. Although the NDPA makes no explicit mention of Artificial Intelligence, this paper argues that the Act remains a relevant and authoritative instrument for the regulation of AI.

Through a detailed analysis of Sections 24, 25, and 37, the paper demonstrates how core principles of data protection — lawfulness, fairness, transparency, accountability, purpose limitation, and the right not to be subject to solely automated decision-making — apply directly to AI systems. The paper concludes that while the NDPA provides a solid foundational layer for AI governance, it is not a comprehensive AI regulation. Nigeria still requires a dedicated, risk-based AI framework to address the unique challenges of generative AI, deepfakes, and high-risk automated systems.

Keywords: Nigeria Data Protection Act, Artificial Intelligence Regulation, Automated Decision-Making, Data Protection, Section 37 NDPA, AI Governance in Nigeria

Introduction

Nigeria's foundational data law, the Nigeria Data Protection Act (NDPA), was enacted in 2023 to serve as the comprehensive rulebook on the processing of personal data within Nigeria and for matters connected to data privacy. The NDPA has 8 listed objectives, two of which are to provide for the regulation of the processing of personal data and to safeguard the fundamental rights and freedoms and interests of data subjects as guaranteed under the Constitution of the Federal Republic of Nigeria 1999 (as amended). Other key objectives worthy of cognizance include the establishment of the Nigeria Data Protection Commission and the fulfilment of the obligations of data controllers towards data subjects.

Since the foundational architecture of artificial intelligence is data, it is expedient to understand how or whether a general-purpose law such as the NDPA applies to it, especially as the race to govern intelligence continues to take the centre stage in many countries. In an attempt to answer the question of whether or not the NDPA is intended for AI, it has been observed that Nigeria lacks an AI specific law and that there is no specific mention of AI in the NDPA 2023. Notwithstanding, it is safe to assume that as long as the rights of data subjects, the processing of personal data and the obligations of data controllers or processors are issues of major importance, the NDPA 2023 is an authoritative instrument of AI regulation.

The absence of an AI specific law addressing data privacy in Nigeria doesn't automatically translate to the absence of regulation and the reference to AI inferred from the joint reading of sections 24, 25 and 37 of the NDPA is neither a technical error of omission nor a fundamental policy flaw. While the need for a local context AI law is one of pressing concern, the fact that the word 'AI' is not mentioned in the NDPA is a genius move to avoid potential ambiguity that

could result from future modification or the invention of new terminologies by the AI community.

Section 24

Section 24(part IV)of the NDPA establishes duty of care and accountability under the heading

Principles Of Personal Data Processing.

The verbatim text of this Section details the foundational principles governing the processing of personal data, is provided below

A Data Controller or Data Processor Shall Ensure that Personal Data is

Processed in a Fair, Lawful and Transparent Manner

- collected for specified, explicit, and legitimate purposes, and not to be further processed in a way incompatible with these purposes
- adequate, relevant, and limited to the minimum necessary for the purposes for which the personal data was collected or further processed
- retained for not longer than is necessary to achieve the lawful bases for which the personal data was collected or further processed
- accurate, complete, not misleading, and, where necessary, kept up to date having regard to the purposes for which the personal data is collected or is further processed and processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing, access, loss, destruction, damage, or any form of data breach.

A data controller and data processor shall use appropriate technical and organisational measures to ensure confidentiality, integrity, and availability of personal data.

Notwithstanding anything to the contrary in this Act or any other law, a data controller or data processor owes a duty of care, in respect of data processing, and shall demonstrate accountability, in respect of the principles contained in this Act.

For the Purposes of Subsection (1) (b)

compatibility of further processing shall be assessed considering

- the relationship between the original purpose and the purpose of the intended further processing,
- the nature of the personal data concerned,
- the consequences of further processing,
- how the personal data has been collected, and
- the existence of appropriate safeguards; and

further processing for archiving purposes in the public interest, scientific, historical research purposes, or statistical purposes shall not be considered to be incompatible with the initial purposes .

Section 25

This subsequent section under part IV of the NDPA 2023 provides the legal basis for the processing of personal data. These are safeguards for data controllers and data subjects. The verbatim text is as follows

Without Prejudice to the Principles Set Out in this Act, Data Processing Shall Be Lawful, where

- the data subject has given and not withdrawn consent for the specific purpose or purposes for which personal data is to be processed; or
- the processing is necessary —
- for the performance of a contract to which the data subject is a party or to take steps at the request of the data subject prior to entering into a contract,
- for compliance with a legal obligation to which the data controller or data processor is subject,
- to protect the vital interest of the data subject or another person,
- for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller or data processor, or
- for the purposes of the legitimate interests pursued by the data controller or data processor, or by a third party to whom the data is disclosed.

Interests in Personal Data Processing Shall not be Legitimate for the Purposes of Subsection (1) (b)(v), where

- they override the fundamental rights, freedoms and the interests of the data subject;
- (b) they are incompatible with other lawful basis of processing under subsection subsection (1)(b) (i)-(iv); or
- the data subject would not have a reasonable expectation that the personal data would be processed in the manner envisaged .

Section 37

This is the most direct section addressing AI. It gives data subjects the right not to be subject to decisions based solely on automated processing (including profiling) that produce legal or similarly significant effects on them (e.g., automated credit scoring, algorithmic hiring). Exceptions apply if human intervention is present, or if the decision is required by a contract or authorized by law.

A data subject shall have the right not to be subject to a decision based solely on automated processing of personal data, including profiling, which produces legal or similar significant effects concerning the data subject.

Subsection Shall not Apply, where the Decision is

- necessary for entering into or the performance of a contract between the data subject and a data controller;
- authorised by a written law, which establishes suitable measures to safeguard the fundamental rights and freedoms, and the interests of the data subject; or (c) authorised by the consent of the data subject.

The Data Controller Shall Implement Suitable Measures to Safeguard the Data Subject's Fundamental Rights, Freedoms And Interests, Including the Rights to

- obtain human intervention on the part of the data controller;
- express the data subject's point of view; and
- contest the decision⁶.

Application of the NDPA in the Femi Falana Case

The Femi Falana v Meta Platforms Inc case (Suit No. LD/18843MFHR/2025) provided the first major judicial test of the NDPA's application to AI-generated content. The Lagos State High Court relied heavily on Sections 24 and 37 of the NDPA, together with Section 37 of the 1999 Constitution, to hold Meta liable. The court determined that Meta was a joint data controller and had breached its obligations by allowing the processing and dissemination of inaccurate and harmful personal data through a deepfake video. This judgment confirms that, even without specific AI provisions, the NDPA can be creatively and effectively applied to address certain AI harms.

Conclusion

The Femi Falana, SAN v Meta Platforms Inc case serves as a powerful illustration of both the potential and the limitations of the Nigeria Data Protection Act 2023 in regulating artificial intelligence. By successfully holding Meta accountable under Sections 24 and 37 of the NDPA, coupled with Section 37 of the 1999 Constitution, the judgment affirms that the Act is not irrelevant to AI. Its principles of fairness, accountability, transparency, and protection against solely automated decisions provide a solid foundation for addressing some AI-related harms.

However, the NDPA was not designed as an AI-specific law. Its technology-neutral approach, while forward-looking, leaves significant gaps in addressing generative AI challenges such as deepfakes, synthetic media labelling, high-risk system governance, and systemic platform accountability. The Falana case, though groundbreaking, also revealed the reactive and limited nature of current remedies. Nigeria stands at a critical juncture. The NDPA 2023 should be preserved as 6 37(1)–(3). This provision mirrors Article 22 of the EU General Data Protection Regulation (GDPR), the cornerstone of data protection, but it must be supplemented with a comprehensive, risk-based AI regulatory framework. Such legislation would not only strengthen the enforcement of rights demonstrated in the Falana case but also position Nigeria as a leader in responsible AI governance in Africa. The question is no longer whether the NDPA regulates AI — it does, to an extent — but whether Nigeria is willing to go beyond general data protection to meet the demands of the AI era.

Foot Notes

- Nigeria Data Protection Act 2023.
- NDPA 2023, s 1.
- ss 24, 25 and 37.
- 24(1)–(4).
- 25(1)–(2).
- Nigeria currently lacks a comprehensive AI-specific legislation as at June 2026. The National Digital Economy and E-Governance Bill, which contains provisions on AI, is still under legislative consideration.
- See also the European Union Artificial Intelligence Act 2024, which adopts a risk-based approach going beyond general data protection rules.