# Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2025 – ISSN 2582-7820

Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey




# Safeguarding Data Privacy in the Age of Artificial Intelligence in Nigeria: A Regulatory Perspective


Dr. Moses Peace Richard[a]

[a]Barrister and Solicitor, Supreme Court of Nigeria, Nigeria



*Received* 04 September 2025; *Accepted* 04 October 2025; *Published* 07 October 2025



*As Artificial Intelligence (AI) systems increasingly process vast amounts of personal data, concerns about data privacy, security, and regulatory oversight have emerged. Despite the enactment of the Nigeria Data Protection Act 2023 (NDPA 2023) and other sectoral regulations, AI-specific privacy issues such as algorithmic bias, unauthorised data processing, and opacity in automated decision-making persist. This paper examines the effectiveness of the existing Nigerian data protection regime in curbing the privacy issues associated with AI data processing. By relying on international regulatory models like the European Union's General Data Protection Regulation (GDPR Regulation (EU) 2016/679) and the EU Artificial Intelligence Act 2024, the paper proposes key regulatory strategies, including the adoption of AI-specific policies, transparency mechanisms, and robust accountability measures. It emphasises the need for a balanced regulatory framework that promotes technological innovation while protecting individuals' rights to privacy. Ultimately, ensuring data privacy in AI applications requires a multi-dimensional approach involving policymakers, regulatory agencies, and AI developers. This study postulates that a robust, AI-inclusive regulatory framework is crucial in mitigating privacy risks and ensuring Nigeria's alignment with global data protection standards in the evolving AI landscape. Methodologically, the study utilises a doctrinal legal research approach, critically evaluating statutory provisions, regulatory instruments, and judicial decisions. It further adopts a comparative law methodology, drawing on the European GDPR Regulation (EU) 2016/679 and the EU Artificial Intelligence Act to suggest reforms for Nigeria.*



**Keywords:** *artificial intelligence, regulation, data protection, privacy, comparative law, Nigeria.*

## INTRODUCTION

Recently, the global discourses on AI have gained traction due to advancements in computer programming languages, particularly with the advent of virtual assistants such as Chat GPT, Cortana, Apple Siri, and Google Assistant.[1] In Nigeria, UNICON groups launched Omeife AI in 2022, Africa's first humanoid robot.[2] AI technologies have the potential to transform the operational, strategic, and ethical dimensions of organisations in various ways: AI machines can process large amounts of data efficiently, reduce production costs, solve complex tasks accurately and timeously, and streamline decision-making processes.[3] There is a consensus that AI deployment can also be useful in attaining global sustainable development goals in terms of risk management through predictive analytics and cybersecurity.[4] AI is also widely used in various sectors, such as the financial sector to assess risks by digital lenders and banks, and in the medical sector for prompt diagnosis and scanning voluminous medical records.

AI technologies, while pertinent, are not without shortcomings. AI applications, generally, are said to engender several risks and challenges in terms of their application and execution. For instance, there is the issue of data bias and poor training data, which could lead to discrimination and other concerns, such as privacy violations.[5] Some believe that unscrupulous actors can hijack AI systems to perform unauthorised surveillance, violate the right to privacy, or infringe on the rights of minority groups.[6] According to Leiser, some AI languages contain manipulative digital design strategies that are capable of subverting users'

[1] Bill Gates, 'The Age of AI has begun' (*Gates Notes*, 21 March 2023) <https://www.gatesnotes.com/the-age-of-ai-has-begun> accessed 25 March 2025
[2] Tina Abeku, 'Osibanjo Launches Africa's First Humanoid Robot Omeife' *The Guardian Nigeria* (04 December 2022) <https://guardian.ng/news/osinbajo-launches-africas-first-humanoid-robot-omeife/#google_vignette> accessed 24 March 2025
[3] Moses Peace Richard, 'Legal Perspective on the Use of Artificial Intelligence in Corporate Governance in Nigeria: Potentials and Challenges' (2024) 34(48) Journal of Legal Studies 97–118 <https://doi.org/10.2478/jles-2024-0016> accessed 26 August 2025
[4] Gokturk Kalkan 'The Impact of Artificial Intelligence on Corporate Governance' (2024) 18(2) Journal of Corporate Finance Research 17 –25 <10.17323/j.jcfr.2073-0438.18.2.2024.17-25> accessed 26 August 2025
[5] Richard (n 3) 106
[6] David Leslie et al., 'Human Rights, Democracy, and The Rule of Law Assurance Framework for AI systems: A Proposal Prepared for the Council of Europe's Ad Hoc Committee on Artificial Intelligence' (*The Alan Turing Institute*, 2021) <https://rm.coe.int/huderaf-coe-final-1-2752-6741-5300-v-1/1680a3f688> accessed 25 March 2025

autonomy for the benefit of the platform or application, thereby resulting in a serious ethical conundrum.[7]

A key area of concern in the deployment of AI for regulators is AI's implications for privacy and data protection. AI systems rely heavily on vast amounts of data for training, testing, and operation, making personal data a fundamental resource in their functionality. When this data pertains to identifiable individuals, either directly or indirectly, safeguarding their privacy becomes a critical issue. Some heightened risks from AI systems as they relate to data processing include the utilisation of algorithmic languages to uncover personal and private individual data, a lack of transparency in data collection, and the tendency to gather excessive and privacy-intrusive data.[8] These risks further highlight the need for AI systems to adhere to privacy standards as a focal point in regulatory endeavours. Many legal frameworks assess AI compliance based on how well these systems protect individuals' personal information and mitigate risks associated with data processing.

Global efforts to tackle AI privacy issues through policies, regulations, and strategies have since emerged in recognition of the potential dangers associated with AI deployment. For instance, the European Union (EU) has made profound strides by introducing the EU AI Act, which adopts a risk-based approach to AI regulation. This is achieved by allowing the assessment and decommissioning of high-risk AI systems that can fundamentally impact the rights and privacy of individuals, and ensuring that generative AI, such as ChatGPT, adheres to transparency requirements and EU copyright laws. [9] In Africa, efforts to regulate AI are found in the African Union High-level Panel on Emerging Technologies (APET)'s AU-AI Continental Strategy for Africa, which aims to develop a regulatory framework for AI strategy in Africa. [10] In line with this, the African Commission on Human and Peoples Rights

[7] Mark Lesier, 'Psychological Patterns and Article 5 of the AI Act: AI-Powered Deceptive Design in the Systems Architecture and the User Interface' (2024) 1(1) Journal of AI Law and Regulation 5 – 23 <https://doi.org/10.21552/aire/2024/1/4> accessed 26 August 2025

[8] Michael Hilb, 'Toward Artificial Governance? The Role of Artificial Intelligence in Shaping the Future of Corporate Governance' (2020) 24 Journal of Management and Governance 851–870 <https://doi.org/10.1007/s10997-020-09519-9> accessed 26 August 2025

[9] 'EU AI Act: first regulation on artificial intelligence' (*European Parliament*, 08 June 2023) <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence > accessed 26 August 2025

[10] 'The African Union Artificial Intelligence Continental Strategy For Africa' *AUDA-NEPAD* (30 May 2022) <https://nepad.org/news/african-union-artificial-intelligence-continental-strategy-africa> accessed 26 August 2025

(ACHPR) initiated a central point programme and expert consultation on the effect of AI, robotics, and other emerging technologies on the rights of individuals in Africa.[11]

In Nigeria, the constitutional safeguard of the right to privacy as stipulated under the Constitution of the Federal Republic 1999 (as amended) does not contemplate the intricacies and issues associated with the deployment of AI technologies for data processing.[12] Additionally, Nigeria currently lacks a national AI-tailored legislation.[13] This presents significant regulatory lapses in terms of how private data should be processed, regulated, and enforced in the context of AI generative data. Data protection and privacy in Nigeria are governed by the Nigeria Data Protection Act 2023(NDPA 2023), and Nigeria Data Protection Regulation 2011 (NDPR 2011), which limit the exclusive application of automated decision-making processes for the processing of data, including profiling, that results in privacy violations of the data subject without obtaining the consent of the data subject.[14]

Furthermore, data controllers and processors under the NDPA 2023 are mandated to adopt privacy protection and safety measures when processing personal data by ensuring that personal data is processed lawfully, transparently, and openly.[15] To embellish this, the Nigerian Data Protection Commission (NDPC), which is the agency saddled with the responsibility of administering the NDPA 2023, recently unveiled the General Application and Implementation Directives 2024 (GAID) to the NDPA 2023. In line with this, data processors or controllers utilising AI systems are also required to take into consideration the provisions of the NDPA 2023 when processing sensitive data of minors and other vulnerable groups.[16] While the data privacy protection mechanisms of NDPA 2023 are commendable,

[11] 'PRESS RELEASE: Inception Workshop and Experts' Consultation on the Study on human and peoples' rights and artificial intelligence (AI), robotics and other new and emerging technologies in Africa, 08 -09 June 2023 Nairobi, Kenya' (*African Commission on Human and Peoples' Rights*, 08 June 2023) <https://achpr.au.int/en/news/press-releases/2023-06-08/inception-workshop-and-experts-consultation-artificial-intelligence> accessed 25 March 2025

[12] Emmanuel Salami and Iheanyi Nwankwo, 'Regulating the Privacy Aspects of Artificial Intelligence Systems in Nigeria: A Primer' (2024) 1 African Journal on Privacy & Data Protection 220– 247 <https://doi.org/10.29053/ajpdp.v1i1.0011> accessed 26 August 2025

[13] Richard (n 3) 108

[14] Tiwaloa Osazuwa et al., 'REGULATING ARTIFICIAL INTELLIGENCE IN NIGERIA' (*ÆLEX*, 01 July 2024) <https://www.aelex.com/regulating-artificial-intelligence-in-nigeria/> accessed 25 March 2025

[15] Nigeria Data Protection Act 2023, pt V

[16] *Ibid* s 31

there is a nascent literature on how the Act regulates privacy issues relating to AI development and application in Nigeria.

This article analyses the effectiveness of the current data protection regime in Nigeria in terms of addressing the privacy issues posed by AI deployment and application. Against this background, this paper is structured as follows: Section II describes the nature and concept of AI, highlighting some of the privacy issues posed by its autonomy during data processing. Section III highlights the relationship between AI and data privacy and argues that a robust regulatory intervention is imperative to address the privacy issues created by AI deployment. Section IV offers an overview of the Nigerian regulatory landscape of data protection as prescribed by the NDPA 2023 and NDPA 2011, and analyses their effectiveness in preventing potential violations of data privacy and unauthorised access to personal information.

Section V presents the limitations of the regulatory efforts on AI in preventing data privacy violations. Section VI analyses the limited capacity of the provisions of NDPA 2023 and NDPR 2011 to regulate data privacy issues, particularly their inadequacies in ensuring AI transparency and accountability. Section VII considers international AI regulatory initiatives such as the EU AI Act and the possibility of adaptation into the Nigerian regulatory system. This is followed by a recommendation in section VIII: this includes enacting an AI-dedicated legislation that can address the privacy issues highlighted in the article. Section IX summarises the findings of this paper.

## THE CONCEPT OF ARTIFICIAL INTELLIGENCE

Like most terminologies in the field of law, AI is a complex idea that requires a clear and precise conceptualisation to aid in its development and regulation. Ultimately, the ramifications of the concept of AI matter greatly for policy and regulation, as its distinct meaning and connotation can shape how regulations are adapted to respond to evolving technologies and their application. However, establishing a universal definition of AI has been daunting, due to the varying approaches adopted by different actors in terms of its meaning and definition. AI cuts across various disciplines, and it is believed that its meaning varies from industry to industry. The problem with the lack of an agreed-upon definition of AI is that it makes the formulation of policies and regulations somewhat difficult, as there is

no clearly defined scope for the application of laws and regulations. Although, from a regulatory perspective, one of the most commonly cited definitions of the concept of AI is provided by the Organisation for Economic Cooperation and Development (OECD) as follows:

AI is a machine-based system that is capable of influencing the environment by producing an output (predictions, recommendations, or decisions) for a given set of objectives. It uses machine and/or human-based data and inputs to (i) perceive real and/or virtual environments; (ii) abstract these perceptions into models through analysis in an automated manner (e.g., with machine learning), or manually; and (iii) use model inference to formulate options for outcomes. AI systems are designed to operate with varying levels of autonomy.[17]

The above definition is broad enough to capture various dimensions of AI; however, it further emphasises the fact that AI systems have various levels of autonomy and functions, and due to the multi-layered nature of AI, their meaning is being perceived differently by diverse stakeholders and actors. Furthermore, it also suggests that the function, structure, and capabilities of AI systems are not universal. AI systems can be classified by the specific functionality and tasks they are designed to carry out.[18] For instance, there are strong AI systems that operate autonomously, are self-aware, and can perform tasks and solve problems independently. There are also weak AI systems that require human intervention to perform specific tasks.[19]

Some renowned computer scientists and scholars have also attempted to define AI. For instance, John McCarthy, a computer scientist and one of the founders of the discipline of artificial intelligence, defined it as 'the science and engineering of making intelligent machines, especially intelligent computer programmes, related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to biologically observable methods'.[20]

---

[17] 'AI Principles overview' (*OECD*) <https://oecd.ai/en/ai-principles> accessed 07 April 2025
[18] Bernard Marr, 'What is the Difference Between Weak (Narrow) and Strong (General) Artificial Intelligence (AI)?' (*Bernard Marr*) <https://bernardmarr.com/what-is-the-difference-between-weak-narrow-and-strong-general-artificial-intelligence-a> accessed 07 April 2025
[19] *Ibid*
[20] 'What is AI? / Basic Questions' (*Standford University*) <http://jmc.stanford.edu/artificial-intelligence/what-is-ai/> accessed 07 April 2025

Within the legal context, the above definition is generally criticised for failing to capture regulatory and statutory dimensions, which delineate the scope of law and the agency saddled with the responsibility of implementing and enforcing it. There is the argument that the inclusion of legislative text can play both communicative roles (clarifying legislative intents) and performative roles (identifying investing stakeholders with rights and obligations).[21] However, the danger in providing a legislative definition is that when the legal definition is poorly drafted or inflexible, it risks failing to capture and tackle the challenges and issues it was initially intended to address.[22]

There is also the concern of governance misspecification, which entails that where regulation is tailored to a particular technology, it may not anticipate future technological advancement, which may result in a discrepancy between legislative goals and subsequent technological objectives.[23] As a result, an inflexible AI law may be rendered inefficient or counterproductive to its objectives. From an international policy standpoint, the EU AI Act 2024 defines AI as 'a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.'[24]

In Nigeria, efforts to define AI can be found in the National Information Technology Development Agency (NITDA), which drafted a national data strategy that defines AI as 'the creation of intelligent objects that work and react like humans to carry out certain tasks meant for intelligent beings without human intervention'.[25] Contrary to what is obtainable with modern AI systems, this definition suggests that AI technologies do not need human intervention. The above definitions demonstrate that the exact meaning and conceptualisation of AI depend on the metric used to assess different countries' relative

[21] Price Jeanne, 'Wagging, Not Barking: Statutory Definitions' (2013) 60 Cleveland State Law Review 999–1055 <https://scholars.law.unlv.edu/facpub/764> accessed 25 March 2025
[22] Rowena Rodrigues, 'Legal and human rights issues of AI: Gaps, challenges and vulnerabilities' (2020) 4 Journal of Responsible Technology <https://doi.org/10.1016/j.jrt.2020.100005> accessed 10 April 2025
[23] Matthijs M Maas 'Innovation-Proof Governance for Military AI? How I Learned to Stop Worrying and Love the Bot' (2019) 10(1) Journal of International Humanitarian Legal Studies 129–57 <https://doi.org/10.1163/18781527-01001006> accessed 25 March 2025
[24] EU AI Act 2024, art 3(1)
[25] Salami (n 12)

achievement in developing AI systems. This makes it difficult to formulate a universal definition as some tend to describe AIs based on their functionality and others emphasise the outcome of the task, particularly those closely related to human-like performance. The purpose of this article is not to identify the correct definition or structure for AI. Rather, it contemplates that different meanings can be more suitable for specific purposes or particular actors and/or regulatory agencies.

## INTERPLAY BETWEEN DATA PRIVACY AND AI: THE IMPORTANCE OF REGULATION

The use of AI in processing large data has become rampant recently, particularly following the COVID-19 pandemic, where several governments have developed AI-powered systems to aid in carrying out specific automated tasks.[26] AI chatbots and voice assistants, such as Google Assistant and Gemini, rely on voluminous data extracted from organisations and individuals, social media, and networking platforms to source information and to provide automated responses to prompts. A major problem posed by AI to data is the potential violation of privacy, most especially via data infringements and unauthorised access to personal information.[27] In addition, AI presents issues of bias and discrimination in data processing, the facilitation of abusive data practices, and the amplification of misinformation and disinformation, while promoting real-time surveillance capabilities that could exacerbate cyber threats, such as phishing attacks, through the management of malicious links.[28] On the other hand, AI systems can be hijacked and utilised by unscrupulous individuals to perpetuate data privacy breaches and, in some cases, influence decision-making that would be otherwise detrimental to the data subjects.[29]

---

[26] Pragati Agarwal et al., 'Artificial Intelligence Adoption in the Post–COVID–19 New–Normal and Role of Smart Technologies in Transforming Business: A Review' (2024) 15(3) Journal of Science and Technology Policy Management 506-529 <https://www.emerald.com/insight/content/doi/10.1108/JSTPM-08-2021-0122/full/html> accessed 10 April 2025

[27] 'AI and Privacy: The privacy concerns surrounding AI, its potential impact on personal data' *The Economic Times* (25 April 2023) <https://economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms> accessed 10 April 2025

[28] 'The Impact of Artificial Intelligence on Data Protection and Privacy: A Walk-Through Rights of a Data Subject in Africa' (*Collaboration on International ICT Policy for East and Southern Africa (CIPESA)*, May 2024) <https://cipesa.org/wp-content/files/briefs/The_Impact_of_Artificial_Intelligence_on_Data_Protection_and_Privacy_-_Brief.pdf> accessed 10 April 2025

[29] *Ibid*

Data protection laws, including the NDPA 2023, posit that the right to data access mandates that data subjects should be furnished with information, including the rationale for collecting data, the type of data to be collected and the identity of the data controller.[30] In all cases, this would require competent personnel to ensure that adequate measures and precautions are put in place to observe and guarantee the right to access personal data. However, from a regulatory standpoint, the lack of a legal basis or a defective legal basis in collecting data may impact data output negatively: when AI models are trained with unlawfully acquired data, the processing activities and the outcome are also invariably corrupted. This is particularly concerning when personal data is found amongst the voluminous amount of data used in training AI systems. For example, in 2020, Clearview AI, an AI development company, was considered to have utilised about 4 billion photos in training its facial recognition software.[31] Nonetheless, multiple lawsuits relating to data protection breaches were initiated against Clearview AI by data protection agencies in France, Italy, and Greece.[32]

Data protection breaches are mostly found in automated and autonomous AI technologies that require little or no human involvement. For instance, automated decision-making by AI systems that rely on personal data such as race, gender, religion, and ethnicity may be inaccurate due to poor training data that was supplied to the AI software. Given this, Rowena observed that automated decisions have far-reaching implications on human rights and privacy of data subjects, particularly where the non-participation of human beings in decision-making and data processing has the potential to deprive individuals of their rights to freedom, and consequently undermines proper accountability. The view of the author in this paper is that the processing of data should be lawful and rely on a legal basis while adhering to other data processing policies and conditions. This is necessary to ensure that personal data is not subject to unauthorised access and abuse. Furthermore, the availability of a legal basis for data processing by AI will also ensure that developers are adequately held accountable for data infringement occasioned by the AI systems. This was the case in Italy

[30] Nigeria Data Protection Act 2023, ss 24 and 25

[31] Tim Cushing, 'How Much Data Does Clearview AI Gather on People? The Answer (Sadly) Will not Surprise You' (*Techdirt*, 27 March 2020) <https://www.techdirt.com/2020/03/27/how-much-data-does-clearview-gather-people-answer-sadly-will-not-surprise-you/> accessed 10 April 2025

[32] Bill Toulas, 'Clearview Gets Third €20 million Fine for Illegal Data Collection' (*Bleeping Computer*, 21 October 2022) <https://www.bleepingcomputer.com/news/security/clearview-ai-gets-third-20-million-fine-for-illegal-data-collection/> accessed 10 April 2025

when data protection authorities suspended OpenAI and Replika for unlawfully collecting data without putting in place an age verification system for children.[33]

## DATA PRIVACY PROTECTION LANDSCAPE IN NIGERIA: OVERVIEW

Like most other countries, Nigeria has been experiencing rapid digital transformations, leading to an increase in the adoption of smartphones and internet connectivity, with heavy reliance on electronic services that are managed by AI systems. The potential issues of data breaches emanating from the widespread use of AI in Nigeria warrant an investigative approach to the regulatory system governing personal data processing. One vital data protection regulation is the NDPR 2011, which is an instrument of general application for all sectors involved in the processing of personal data. The NDPR is modelled after the EU's General Data Protection Regulation (GDPR), and prescribes provisions on the rights of individuals, the obligations of data controllers and processors, and penalties for non-compliance.

The NDPR was generally criticised for lacking an independent supervisory authority, not having a robust legal basis, and, consequently, having a weak enforcement regime.[34] Consequently, NPDA 2023 was enacted to fill this lacuna in the regulatory system. The Act stipulates a legal framework for safeguarding personal information and establishes the Nigeria Data Protection Commission (NDPC) or Commission) to regulate the processing of personal information. However, the NPDA 2023 did not expressly repeal the NDPR, which means that data processors and controllers must comply with both instruments in the processing of personal data.

Key data protection provisions in the NDPA 2023 can be found in section 40(3), where a personal data breach likely to cause high risk to the rights and freedoms of individuals shall be communicated immediately to the data subject by the data controller, including advice about measures that can be adopted to mitigate effectively the potential adverse effects of

[33] 'Artificial intelligence: the Guarantor blocks chatgpt. Illegal collection of personal data. Absence of systems for verifying the age of minors' (*GPDP*, 31 March 2023) <https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english_version> accessed 10 April 2025

[34] Adekemi Omotubora, 'How (Not) to Regulate Data Processing: Assessing Nigeria's Data Protection Regulation 2019 (NDPR)' (2021) 2(3) Global Privacy Law Review 186-199 <https://doi.org/10.54648/gplr2021024> accessed 10 April 2025

data breaches. Additional safeguard mechanisms are prescribed concerning sensitive personal data processing, such as health, genetic, and biometric data. In this regard, the Act stipulates specific grounds for which data controllers and processors can process sensitive data as follows:

1. Where the data subject has given and not withdrawn consent for the processing activity;
2. Where the processing is necessary for reasons of substantial public interest based on a law, or where the processing is necessary for public health.
3. Where the processing is necessary for the performance of the data controller's obligations or the existing rights of the data subject under employment or social security laws, or any other similar laws;
4. Where the processing is necessary to protect the vital interests of the data subject or another person; and
5. Where the processing is carried out for purposes of medical care or community welfare and undertaken by or under the responsibility of a professional owing a duty of confidentiality.[35]

The implication of the above provisions on AI deployment and use is that data processing must be lawful and carried out in line with the abovementioned prescribed grounds by ensuring that data processing is done for the vital interest of the data subject and in the interest of the public. In terms of AI systems, it also means that AI technologies must be developed to permit data subjects to enforce their rights against data breaches, and rights to information, and not to have their data subjected to scrutiny without giving consent. Section VI will critically examine the efficacy of the NPDA 2023 and NPDR provisions in regulating data privacy during the deployment of AI systems in Nigeria.

## REGULATORY LANDSCAPE OF ARTIFICIAL INTELLIGENCE IN NIGERIA

AI has gained considerable traction in Nigeria, with its application cutting across various sectors of the economy. For instance, AI is being deployed in the financial sector to track and mitigate financial risks and money laundering. Within the health sector, AI is applied to run diagnoses and prognoses on patients, and in the construction sector, AI is being utilised for

[35] Nigeria Data Protection Act 2023, s 30

building designs. Other Key sectors, such as education, agriculture, and sports, are using AI to streamline their organisational systems and, in turn, drive efficiency. The growing application of AI and its potential drawbacks further emphasise the need for regulatory responses, which have been considered abysmal. Nigeria's AI framework is currently in its embryonic stage, lacking a dedicated AI law or regulation.

Although steps have been taken by some Nigerian institutions to proffer a regulatory structure for modern technology. AI is generally considered by the National Digital Economy Policy and Strategy (NDEPS) as an evolving technology that will enhance the Nigerian economy and the lives of its citizens if applied judiciously.[36] Against this backdrop, NITDA established the National Council for Artificial Intelligence and Robotics (NCAIR) as an innovative institution bestowed with the duty of conducting research and understanding the application of emerging technologies like AI, deep learning, augmented realities, robotics, and Internet of Things. In 2022, it began developing an AI policy for Nigeria.

The first draft of the AI policy was completed in March 2023 and forwarded to the Federal Executive Council (FEC) for approval.[37] In August 2023, the Federal Ministry of Communication, Innovation and Digital Economy (FMCIDE) also published a draft National Artificial Intelligence Strategy (NAIS), which provides a roadmap for developing a robust framework that supports ethical and responsible use of AI, intended to mitigate consequent risks.[38] There are four broad risk areas identified by the NAIS: economic, societal, ethical, and AI model. In terms of implementation, it adopted the assess, mitigate, monitor, and review process as prescribed by the National Institute of Standards and Technology AI Risk Management Framework (NIST AI RMF), which was designed to help organisations manage AI risk at every stage of the AI lifecycle.

[36] 'National Digital Economy Policy and Strategy (2020-2030)' (*Federal Ministry of Communications and Digital Economy*, November 2019) <https://nitda.gov.ng/wp-content/uploads/2020/06/National-Digital-Economy-Policy-and-Strategy.pdf> accessed 17 April 2025

[37] Nkechi Isaac, 'FG Finalises Policy on AI, Commends Volunteers for Contributions' (*Science Nigeria*, 08 March 2023) <https://sciencenigeria.com/fg-finalises-policy-on-ai-commends-volunteers-for-contributions/> accessed 21 April 2025

[38] Jeffrey Shin and Cameron Lee, 'AI Watch: Global Regulatory Tracker – Nigeria' (*White & Case LLP*, 27 January 2025) <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-nigeria> accessed 21 April 2025

In an attempt to drive AI innovation in Nigeria, FMCIDE also hinted at its strategy on IA by publishing a white paper, which recognised the multifaceted and complex nature of AI, specifically highlighting its economic and social benefits to the economy. Given this, FMCIDE has already compiled a list of AI researchers who will assist in building innovative technological solutions, in view of solving national problems and creating job opportunities for citizens. Undoubtedly, these are commendable steps, although none of the initiatives have resulted in a solid framework for AI in Nigeria, which caters to data privacy issues. It is generally observed that other factors that could impede the implementation of a robust AI system in Nigeria are insufficient funding, a lack of an expert workforce, and ethical and data security concerns, which could lead to a slow adoption by the private sector.

## PRIVACY AND DATA PROTECTION ISSUES RELATING TO AI DEPLOYMENT IN NIGERIA

As Nigeria struggles to grapple with the rapid evolution of AI, the relationship between technology and data protection becomes increasingly important. The rapid progress of AI raises key data privacy issues associated with how personal data is collected, processed, and safeguarded by the existing laws on data protection. The challenge lies in striking the right balance between offering AI-driven solutions and guaranteeing citizens' rights to privacy and data safety. In particular, data protection issues relating to the utilisation of AI generally are said to be present throughout the lifecycle of AI, from its development stage to its deployment stage. Data bias as a result of poor training algorithms during the machine learning stage, privacy violations during the collection and processing of data, poor quality of data, and lack of transparency and algorithmic accountability due to automated decision-making are commonly cited AI problems that require adequate regulatory responses. This section critically assesses the legal capacity of the NDPA 2023 and NDPR 2011 in addressing these issues in Nigeria.

**Data Breach:** Data collection is the basis of AI development, and where such a process is done unethically and without a proper legal basis, the propensity for data breaches and corrupted data output becomes imminent. Data breaches in the development of AI can occur in various forms, mostly due to insufficient data protection measures and unethical practices during the data collection stage. For instance, some AI developers rely on web scraping,

which is a technique used to automatically extract data from websites using software.[39] This technique is usually unlawful as it lacks a legal basis in terms of data collection during AI development.[40]

Most data protection laws, including the NDPA 2023, require that data collection must be carried out lawfully and in compliance with legal obligations.[41] In this regard, the NDPA 2023 offers an interim protection for data subjects against potential violations by data controllers during the collection stage. Thus, where AI developers unlawfully collect data, this will result in the breach of the privacy rights of data subjects. Invariably, the affected data subject can seek redress under the NPDA for unlawful data processing. Section 25(b)(iii) went further to provide that data processing must be carried out to protect the interests of the data subject. This ensures that data controllers or AI developers take measures to ensure that data collection does not prejudice the interests of the data subject. While not expressly stated, it is apposite to state that the NPDA 2023 offers some notable provisions that militate against the abuse of data during the deployment stage of AI.

**Inadequate Transparency in Data Processing:** The algorithmic nature of AI systems generally makes it difficult to understand how they reach a decision or the rationale behind their decision, thereby hindering transparency and accountability. This issue is commonly known as the 'black box' problem, which arises when AI models make decisions without clear, understandable reasoning. While AI technologies offer precision in decision-making, their opacity can erode trust, fairness, and accountability. For instance, a hiring algorithm may reject a candidate but fail to offer the factors that led to the rejection. Likewise, a medical diagnostic software might suggest a particular treatment without stating its rationale. Transparency is therefore crucial because it cuts across the entire life cycle of AI.

There are no specific provisions in the NDPR 2019 regarding the transparency of AI. Although it can be inferred from the principles in section 3.1. about data subjects' right to be furnished with 'any information relating to processing in a concise, transparent, intelligible and easily accessible manner using clear and plain language'. Furthermore, NDPR 2019

[39] Will Hillier, 'What Is Web Scraping? A Complete Beginner's Guide' (*Career Foundry*, 13 August 2021) <https://careerfoundry.com/en/blog/data-analytics/web-scraping-guide/> accessed 21 April 2025
[40] *Ibid*
[41] Nigeria Data Protection Act 2023, s 25(1)

stipulates that before the commencement of the processing activity, data subjects are to be provided with transparent information. NDPA 2023 went further to state that the data controller or processor must ensure that personal data is processed in a fair, lawful, and transparent manner.

The implication of this is that AI developers must ensure that their systems are designed in a manner whereby the algorithm can clearly explain the reason behind the output, making the decision accessible and comprehensible. To further embellish the requirement for transparency, section 27 of the NDPA 2023 enumerated the information that must be afforded to a data subject, which *inter alia* includes the existence of automated decision-making, including profiling, the significance and envisaged consequences of such processing for the data subject and the right to object to and challenge such processing.

This provision is significant because it addresses a key transparency issue presented by AI systems that are equipped with automated decision-making capabilities. As stated above, some AI systems may make decisions expressly, without furnishing reasons for their decisions. In congruence with section 27 of the NDPA 2023, a data subject can decide how their data should be collected and processed, and possibly refuse to give consent to such data processing.

However, in practice, the application of this provision may prove difficult because of the black-box nature of AI systems, most especially, AI technologies that process information without human input. For instance, facial recognition cameras are generally designed to capture images of individuals automatically and in real time without the consent of the data subject. In such circumstances, it is noted that due to the automated, spontaneous, and large-scale nature of the data collection with facial recognition software, it is usually impractical for one to obtain transparent information about the data subject.

**Data Bias:** When the data used in training AI models contains inaccurate, skewed, or incomplete information, data bias becomes inevitable. Such bias usually occurs at the processing or pre-processing stage of the AI development. This can lead to systematic errors in the prediction or decision-making by AI technologies. For example, if the data used for the training of a facial recognition system is largely based on pictures of individuals from a specific ethnic group, it may struggle in detecting faces of people from other ethnic

backgrounds. This can result in misidentification or discrimination against a certain group due to poor quality of training data. It is recommended that one technique to tackle this issue is to ensure that training data are meticulously curated and processed, while ensuring that underrepresented groups are oversampled.

In Nigeria, the requirements regarding the quality of data can be found in the NDPR and NDPA, respectively. Section 24(1)(e) of the NDPA 2023 provides 'that a data controller or data processor shall ensure that personal data is accurate, complete, not misleading and where necessary, kept up to date having regard to the purpose for which the personal data is collected or is further processed.'[42] This provision is vital in terms of addressing data bias issues in AI development because it will ensure that AI technologies in Nigeria are created with high-quality data, which would not lead to bias or discrimination. Consequently, using poor-quality or inaccurate data in the training of an AI algorithm will result in infringement of the NDPA.

**Lack of Algorithmic Accountability:** The growing application of AI systems in businesses and government institutions in Nigeria raises the question of accountability. Who should be held accountable when AI systems malfunction and create negative outcomes: the developers, the organisation, or the AI itself? This is relevant in sectors like health and insurance, where AI algorithms are increasingly applied to make decisions that can affect the lives of citizens. For instance, AI technologies are gradually being applied by financial institutions in Nigeria to ascertain the eligibility of individuals for loan facilities.[43] While the NDPA and NDPR contain useful provisions that guarantee data quality and accuracy when using AI systems, they seem to lack clear accountability measures for addressing situations where decisions are made incorrectly due to poor-quality training data. In such a situation, the lack of proper accountability measures can impede regulators from adequately determining who should be held accountable for the malfunctioning of an AI system that leads to a gross breach of an individual's privacy. Invariably, this also leaves AI providers and deployers completely unaccountable to individuals harmed by AI systems if they fail to

[42] Nigeria Data Protection Regulation 2011, s 2.1.(1)(b)
[43] Terhile Ikyo, 'Emerging Issues for Nigerians in the Age of Artificial Intelligence' *Vanguard* (07 October 2024) <https://www.vanguardngr.com/2024/10/emerging-issues-for-nigerians-in-the-age-of-artificial-intelligence/> accessed 30 April 2025

take appropriate measures.[44] It is clear from this that NDPA and NDPR were not specifically tailored to cater for AI data processing and the accountability issues that affect the development and deployment of AI technologies.

In comparison, the EU AI Act addresses the accountability gap by introducing the concept of 'provider accountability.' In this regard, the Act holds developers and manufacturers accountable for the failure of AI systems, whether intended or not.[45] It is argued that this approach is too rigid and unfair to small and medium-sized companies, which would struggle to manage the liability burden that will attach itself to AI development. [46] On this basis, it is recommended that a more suitable approach would be to regulate AI not as a single product or service but as a continuous process that regularly undergoes amendments and adaptations. [47]

## INTERNATIONAL INITIATIVES ON DATA PRIVACY PROTECTION IN AI SYSTEMS: LESSONS FOR NIGERIA

The EU is one of the regions that has made significant strides concerning data protection in terms of AI regulation. For instance, the EU AI system is generally governed by the General Data Protection Regulation 2016 (GDPR 2016), which was adopted by the European Parliament and Council of the European Union and entered into force on the 25th of May 2018. More recently, the EU also enacted the EU Artificial Intelligence Act 2024 (EU AI Act 2024), which is generally considered a transformative piece of legislation for data protection within the era of AI. In light of privacy protection, the GDPR accords data subjects the right to information and not to be subjected to a decision based solely on automated processing, including profiling.[48] For data privacy protection, both instruments are keen on ensuring that adequate accountability and transparency are maintained during the deployment of AI systems.

---

[44] *Ibid*

[45] Laura Lazaro Cabrera, 'Effective Remedies in AI: An Insufficiently Explored Avenue for AI Accountability' (*Center for Democracy and Technology*, 14 November 2024) <https://cdt.org/insights/effective-remedies-in-ai-an-insufficiently-explored-avenue-for-ai-accountability/> accessed 30 May 2025

[46] 'Accountability in the EU AI Act: Who is Responsible for Decisions Made by AI?' (*Access Partnership*, 17 February 2022) <https://accesspartnership.com/accountability-in-the-eu-ai-act-who-is-responsible-for-decisions-made-by-ai/> accessed 30 May 2025

[47] *Ibid*

[48] General Data Protection Regulation (GDPR) 2016, arts 12, 13, 14 and 22

The GDPR implements this through requirements such as the information obligation and the right to information in art. 13 and 14, respectively. In this regard, GDPR allows the data subject to be informed of the circumstances of the data collection. Thus, the provision mandates the data controller to provide *inter alia*, the name and contact details of the data controller and the purpose and legal basis of processing of the personal data; the recipient or categories of recipient of the personal data; the controller's intention to transfer the data to (recipient) a third country or international organisation.[49] This provision is significant to data privacy protection in the AI deployment context because it ensures that developers and users of AI systems adequately inform data subjects of the reason for using their data, irrespective of whether the data is obtained from the data subjects themselves or third parties. Thus, where the data controllers fail to comply with this, they may be liable for a fine or sanctions.

The EU AI Act also contains noteworthy provisions relating to data privacy protection. For this, it adopts a risk-based approach to AI systems, stipulating obligations to data controllers and processors depending on the risk level of the AI technology. To attain this, the Act classifies AI systems into four risk categories: prohibited risk, high risk, limited risk, and minimal risk. The prohibited risks are unacceptable AI systems and are not allowed. This includes AI that can manipulate human behaviours and/or use real-time remote biometric identification like facial recognition software in public spaces and for social scoring.[50] High-risk AI systems are those in human resources and law enforcement, and are subject to strict regulation, while minimal risk AI systems are not regulated at all.[51] Lastly, limited risk AI is subject to lighter transparency obligations and includes chatbots and systems that generate or manipulate content such as video and audio. According to Chapters 4 and 5 of the EU AI Act, those who utilise high-risk or limited risk AI systems must conduct thorough evaluation and testing before deployment, and must ensure that AI-generated or modified content (eg, deep fakes) is clearly labelled as such.[52]

---

[49] *Ibid* arts 13 and 14

[50] Daniel Gonzalez Riedel and Stephan Idema, 'Understanding Intersection Between EU's AI Act and Privacy Compliance' (*Compact*, 12 September 2024) <https://www.compact.nl/articles/understanding-intersection-between-eus-ai-act-and-privacy-compliance/> accessed 29 June 2025

[51] Martin Röleke, 'GDPR and AI Act: Similarities and Differences' (*Active Mind Legal*, 16 October 2024) <https://www.activemind.legal/guides/gdpr-ai-act/> accessed 29 June 2025

[52] 'A Comprehensive EU AI Act Summary [Aug 2025 update]' (*Software Improvement Group*, 14 August 2025) <https://www.softwareimprovementgroup.com/eu-ai-act-summary/> accessed 29 June 2025

The OECD has also spearheaded AI policies in an attempt to safeguard against privacy violations and to protect personal data. Given this, the OECD in 2019 published the Principles on Artificial Intelligence (OECD AI Principles) to promote AI systems that are innovative, trustworthy, and respect human rights and democratic values. This is in line with NDPA 2023, which also mandates data controllers to establish appropriate measures to safeguard the data subjects' fundamental rights, freedom, and prevent violations of their privacy and rights to contest automated decisions.[53] This provision is very useful because AI systems and algorithms are usually affected by margins of error. The availability of such provisions would mean that AI technologies are developed and deployed in ways that would afford data subjects the right to enforce their privacy rights against the unlawful collection and processing of their data.

In terms of data protection, the OECD AI principles provide that there should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them. This principle is in line with modern AI policies, which emphasise the need for transparency in the processing of personal data with the aid of AI systems. With regards to transparency, the NDPA 2023 only contains provisions that afford a data subject the right not to be subjected to an automated decision. However, it fails to stipulate provisions that allow data subjects to be provided with meaningful information about the reasoning behind an automated decision relating to them.

The NDPR 2011 fills this gap by affording data subjects the right to receive an explanation for automated decisions that affect them.[54] On the other hand, NDPR does not expressly prescribe provisions that afford data subjects the right to refuse to be subjected to an automated decision. Against this background, it is clear that both regulatory instruments are complementary and should be applied conjunctively to ensure that data privacy is adequately safeguarded in the development and deployment of AI systems in Nigeria, where the NDPR falls short, the NDPA 2023 appears to fill the gaps, and vice versa.

[53] Nigeria Data Protection Act 2023, s 37(3)
[54] Nigeria Data Protection Regulation 2019, s 3.1(7)(L)

## RECOMMENDATIONS

From the above, it is clear that the NDPA 2023 and NDPR 2019 were not specifically designed to cater to the complex and evolving issues posed by AI systems. At this juncture, a holistic regulatory approach is imperative to enhance the regulatory framework governing privacy in Nigeria's AI environment. To ensure responsible AI practices and to bolster the protection of data privacy, the following measures are recommended for Nigeria:

**Development of AI-Specific Legislation:** It is postulated that the lack of specific AI legislation in Nigeria may hinder the effective regulation of the development and deployment of AI in Nigeria. Although data privacy issues relating to AI in Nigeria can be fairly tackled using existing data protection laws, such as the NDPA and NDPR, these legislations, as demonstrated earlier, have certain limitations. It is the recommendation in this paper that the Nigerian government should enact specific AI laws that can adequately address the challenges posed by AI technologies by incorporating provisions for algorithmic transparency, accountability, and ethical AI deployment. The proposed AI law should be modelled after the EU AI Act 2024, which is generally considered a global model for other regions to follow. Similar to the EU AI Act, the proposed law should adopt a risk-based approach to AI by categorising AI systems based on their risk level. As shown above under the EU AI Act, AI systems are classified into prohibited, high, limited, and minimal risk. This categorisation is useful in ensuring that the law is specifically tailored to address unique challenges that are presented by various AI systems. As highlighted above, there are both weak and strong AI systems: the strong AI systems, which are more complex, require greater regulation, whereas weak AI systems may not require stringent regulation as they tend to pose lesser risks.

Ultimately, the challenges created by AI systems are universal. Therefore, a framework for regulating AI technologies in Nigeria should be proactive, ethical, and risk-based. Taking a risk-based approach to regulation, as stipulated in the EU AI Act, would also ensure that Nigeria aligns itself with global best practices, which will put Nigeria in a position to effortlessly export its AI technology responsibly and ethically. Undoubtedly, the success of AI applications in Nigeria is dependent predominantly upon the legal armoury established

to tackle the convoluted legal, ethical, and social issues that emanate during their development and deployment.

**Algorithmic Transparency and Accountability:** In addition to introducing a national AI law, there is a need to ensure that the policies promote adequate algorithmic accountability and transparency in the processing of sensitive data. AI developers should be required to provide information about how their algorithms work, including the data they use and the reasons for the decisions they make. As explained above, the Nigerian data protection framework currently lacks clear mechanisms for holding AI developers and programmers accountable for the harmful outcomes of AI systems. Furthermore, the NDPA 2023's lack of clear mechanisms mandating AI systems to provide reasons for their decisions also undermines transparency in the application of AI technology for personal data processing in Nigeria. It is recommended here that the proposed AI laws should contain provisions that mandate clear explanations of AI-driven automated decisions, particularly when they impact individuals' rights.

**Enhanced AI Law Enforcement:** Laws without adequate enforcement are generally considered ineffective in addressing the issues they were initially enacted to tackle. In Nigeria, weak enforcement is widely seen as one of the problems plaguing most digital laws, with the lack thereof undermining compliance.[55] It is argued that regulatory intervention through principles and robust enforcement action is essential in securing compliance. With AI applications, the enforcement of the conditions of data protection should be the focus of Nigeria's data protection framework. The enforcement mechanism should promote lawful data processing, particularly in the early stages of AI development. This will ensure that the legal basis for data processing requirements is adhered to while empowering regulatory agencies with the authority and resources to monitor and enforce AI deployment, and to ensure compliance with data protection standards.

## CONCLUSION

While the emergence of AI presents transformative opportunities for Nigeria's digital economy, it simultaneously exposes significant weaknesses in the protection of personal

[55] Hembadoon Orsar, 'Expert Blame Weak Enforcement for Digital Rights Violation' *Leadership* (31 March 2025) <https://leadership.ng/experts-blame-weak-law-enforcement-for-digital-rights-violation/> accessed 25 August 2025

data. Though strengthened by the NDPA and NDPR, the existing regulatory framework remains insufficient in addressing complex AI privacy issues, such as inadequate algorithmic accountability, data minimisation, and transparency in automated decision-making. In line with global standards such as the GDPR and the EU AI Act, effective AI governance in Nigeria requires general data protection laws that promote transparency, privacy, and accountability. Nigeria must therefore prioritise the development of AI-specific laws that are adaptable, enforceable, and rooted in human rights principles. This includes fostering collaboration among regulators, technology developers, and policymakers to ensure inclusive policymaking and compliance. Ultimately, the sustainability of AI in Nigeria depends on a forward-looking regulatory strategy that balances innovation with the imperative to protect individual privacy in the digital age.