

## ARTIFICIAL INTELLIGENCE IN NIGERIA: LEGAL AND ETHICAL IMPLICATIONS FOR A DEVELOPING DIGITAL STATE

**Bamikole A. P. Folorunso\***

### **Abstract**

*Artificial Intelligence (AI) is rapidly transforming governance, economic systems, and regulatory environments across the Global South. Nigeria's accelerated adoption of AI technologies driven by digitalisation initiatives and expanding data ecosystems has created significant legal and ethical challenges that existing regulatory frameworks are not equipped to manage. This article provides a doctrinal, comparative, and practice-oriented analysis of the legal and ethical implications of AI deployment in Nigeria, focusing on data protection, privacy, algorithmic bias, discrimination, and others. Using applicable legal framework as analytical anchors, the study identifies substantial governance gaps arising from fragmented legislation, weak enforcement capacity, among others within comparative models. It proposes the enactment of a dedicated AI Governance Act, the establishment of an independent AI regulatory among other recommendations. The study concludes that Nigeria's AI trajectory must be guided by human-centred, ethical, and future-ready regulatory principles to ensure responsible innovation and sustainable digital development.*

**Keywords:** AI Governance; AI Policy in Africa; AI Regulation; Algorithmic Bias; Automated Decision-Making

---

\* Lecturer, Faculty of Law, Feritas University Abuja, PhD Candidate,

## 1.0 INTRODUCTION

Artificial Intelligence (AI) has emerged as one of the most transformative technologies of the twenty-first century, reshaping global economic systems, governance structures, and social interactions. Its capacity to automate decision-making, analyse vast datasets, and perform tasks traditionally associated with human cognition has accelerated its adoption across sectors such as healthcare, finance, agriculture, transportation, security, and public administration. Nigeria has similarly embraced AI-driven technologies, supported by initiatives such as the National Centre for Artificial Intelligence and Robotics (NCAIR) and the ongoing development of a National Artificial Intelligence Strategy (NAIS). These developments reflect the country's ambition to leverage AI for socio-economic transformation and digital competitiveness.<sup>1</sup>

However, as I have observed in my professional capacity as a Data Protection Officer and legal practitioner, the rapid integration of AI into critical sectors raises profound legal, ethical, and governance challenges. AI systems rely heavily on large-scale data processing, heightening concerns about privacy, data protection, and the potential misuse of personal information. Nigeria's primary data governance instruments—the Nigeria Data Protection Regulation (NDPR) 2019 and the Nigeria Data Protection Act (NDPA) 2023 provide foundational safeguards, but they remain limited in scope, enforcement, and alignment with global standards such as the European Union's General Data Protection Regulation (GDPR).<sup>2</sup> Similarly, while the Cybercrimes (Prohibition, Prevention, etc.) Act 2015 establishes mechanisms for cybersecurity

---

<sup>1</sup> National Information Technology Development Agency (NITDA), *National Artificial Intelligence Strategy (Draft)* (2023).

<sup>2</sup> Nigeria Data Protection Act 2023; Regulation (EU) 2016/679 (General Data Protection Regulation).

and the protection of digital infrastructure, it does not address the unique risks posed by autonomous and algorithmic systems.<sup>3</sup>

Beyond data governance, AI deployment raises ethical concerns relating to algorithmic bias, discrimination, opacity in automated decision-making, and accountability gaps associated with autonomous systems. These risks are particularly acute in developing countries, where weak institutional capacity, limited technological literacy, and socio-economic inequalities may exacerbate the harms associated with AI. Nigeria currently lacks a codified ethical framework for AI, and existing regulatory institutions face significant constraints in monitoring and enforcing responsible AI practices.<sup>4</sup>

Internationally, several governance models have emerged to guide the ethical and legal deployment of AI. These include the OECD Principles on Artificial Intelligence, UNESCO's Recommendation on the Ethics of Artificial Intelligence, and the European Union's Artificial Intelligence Act, which adopts a risk-based regulatory approach.<sup>5</sup> These frameworks provide valuable benchmarks for Nigeria as it seeks to develop a coherent and context-appropriate AI governance regime.

Against this backdrop, this article undertakes a doctrinal and practice-oriented analysis of the legal, ethical, and regulatory imperatives for responsible AI governance in Nigeria. It examines existing legislation, policy instruments, and institutional mechanisms; interrogates the adequacy of current safeguards; and draws comparative

---

<sup>3</sup> Cybercrimes (Prohibition, Prevention, etc.) Act 2015.

<sup>4</sup> Anna Jobin, Marcello Ienca and Effy Vayena, 'The Global Landscape of AI Ethics Guidelines' (2019) 1 *Nature Machine Intelligence* 389.

<sup>5</sup> European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)* COM(2021) 206 final; OECD, *OECD Principles on Artificial Intelligence* (2019); UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

insights from global regulatory models. The study argues that Nigeria requires a more integrated, adaptive, and rights-respecting governance framework capable of addressing the multifaceted risks associated with AI while enabling innovation and sustainable development.

## **2.0 LEGAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE IN NIGERIA**

Artificial Intelligence introduces a range of complex legal challenges that cut across data protection, privacy, discrimination, liability, cybersecurity, and administrative justice. As AI systems increasingly influence decision-making in both public and private sectors, existing Nigerian laws—many of which were designed for earlier generations of digital technologies—struggle to address the unique risks posed by autonomous and algorithmic systems.<sup>6</sup> Global scholarship has highlighted the need for adaptive legal frameworks capable of responding to the opacity, unpredictability, and scale of AI-driven processes.<sup>7</sup> This section examines the major legal implications of AI within the Nigerian context, identifying the gaps, challenges, and emerging regulatory needs that must be addressed to ensure responsible and rights-respecting AI deployment.

### **2.1 Data Protection and Privacy Concerns**

AI systems rely heavily on the collection, processing, and analysis of large datasets, often containing personal or sensitive personal information. In Nigeria, the primary legal framework governing data protection is the Nigeria Data Protection Act (NDPA) 2023, which replaced the earlier Nigeria Data Protection Regulation (NDPR) 2019.

---

<sup>6</sup> Nigeria Data Protection Act 2023; Cybercrimes (Prohibition, Prevention, etc.) Act 2015; NITDA Act 2007.

<sup>7</sup>Frank Pasquale, *The Black Box Society* (Harvard University Press 2015); Solon Barocas and Andrew Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.

The NDPA establishes principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, and accountability.<sup>8</sup> These principles are essential for regulating AI systems, which frequently operate through opaque data-driven processes.

However, the NDPA does not contain AI-specific provisions addressing automated decision-making, profiling, or algorithmic transparency. This creates a regulatory gap, particularly in sectors such as financial services, healthcare, and public administration, where AI-driven decisions may significantly affect individuals' rights. For instance, automated credit-scoring systems may deny loans without providing meaningful explanations, thereby undermining the right to fair hearing and due process.<sup>9</sup>

Furthermore, Nigeria lacks a statutory right to explanation comparable to Article 22 of the GDPR, which grants individuals protection against decisions based solely on automated processing.<sup>10</sup> The absence of such safeguards exposes Nigerians to potential harms arising from opaque AI systems, including discrimination, unfair treatment, and violations of informational privacy.

## **2.2 Algorithmic Bias and Discrimination**

Algorithmic bias is a significant legal and ethical concern in AI deployment. Bias may arise from skewed training datasets, flawed model design, or systemic inequalities embedded in historical data.<sup>11</sup> In Nigeria, where socio-economic disparities, ethnic diversity, and gender

---

<sup>8</sup> Nigeria Data Protection Act 2023, ss 24–32.

<sup>9</sup> Olumide Adeyemi, 'Automated Decision-Making and Due Process in Nigeria's Financial Sector' (2022) 14 *Nigerian Journal of Commercial Law* 55.

<sup>10</sup> Regulation (EU) 2016/679 (General Data Protection Regulation), art 22

<sup>11</sup> Solomon Barocas and Andrew D. Selbst, 'Big Data's Disparate Impact' (2016) 104 *California Law Review* 671.

inequalities are pronounced, biased AI systems may disproportionately harm vulnerable groups.

For example, facial recognition technologies have been shown globally to exhibit higher error rates for darker-skinned individuals and women.<sup>12</sup> If deployed in Nigeria for security or identity verification purposes, such systems could lead to wrongful arrests, exclusion from essential services, or discriminatory profiling. Similarly, AI-driven recruitment tools may inadvertently favour candidates from certain socio-economic backgrounds, perpetuating inequality in employment opportunities.<sup>13</sup>

Nigeria's Constitution prohibits discrimination on grounds of ethnicity, sex, religion, or social status,<sup>14</sup> yet existing legislation does not explicitly address algorithmic discrimination. The absence of AI-specific anti-discrimination provisions creates uncertainty regarding liability, redress, and enforcement. This underscores the need for a comprehensive AI governance framework that incorporates fairness, equality, and non-discrimination principles.

### **2.3 Opacity and Automated Decision-Making**

AI systems, particularly those based on machine learning, often operate as “black boxes,” making it difficult to understand how decisions are reached.<sup>15</sup> This opacity poses challenges for accountability, transparency, and due process. In sectors such as healthcare, policing,

---

<sup>12</sup> Joy Buolamwini and Timnit Gebru, ‘Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification’ (2018) 81 *Proceedings of Machine Learning Research* 1.

<sup>13</sup> Reuben Binns, ‘Fairness in Machine Learning: Lessons from Political Philosophy’ (2018) 81 *Proceedings of Machine Learning Research* 149.

<sup>14</sup> Constitution of the Federal Republic of Nigeria 1999 (as amended), s 42.

<sup>15</sup> Frank Pasquale, *The Black Box Society* (Harvard University Press 2015).

and financial services, opaque AI systems may undermine public trust and hinder effective oversight.

Nigeria's legal system emphasises transparency and accountability in administrative decision-making, yet these principles are difficult to enforce when decisions are made by autonomous systems.<sup>16</sup> Without statutory obligations for explainability or auditability, individuals affected by AI-driven decisions may have limited avenues for contesting or understanding such outcomes.

## **2.4 Liability and Accountability for Autonomous Systems**

Determining liability for harms caused by autonomous AI systems presents complex legal challenges. Traditional liability frameworks such as negligence, product liability, and vicarious liability are premised on human agency and may not adequately address scenarios where AI systems act independently.<sup>17</sup>

For instance, if an autonomous drone used for agricultural monitoring malfunctions and causes property damage, it is unclear whether liability should rest with the manufacturer, software developer, operator, or data provider. Similarly, in the context of autonomous vehicles, questions arise regarding the allocation of responsibility between drivers, manufacturers, and AI developers.<sup>18</sup>

Nigeria currently lacks statutory provisions addressing AI-specific liability. This regulatory vacuum may hinder innovation, as developers and investors may be reluctant to deploy AI technologies without clear

---

<sup>16</sup> Constitution of the Federal Republic of Nigeria 1999 (as amended), s 36.

<sup>17</sup> Margot Kaminski, 'The Right to Explanation, Explained' (2019) 34 *Berkeley Technology Law Journal* 189.

<sup>18</sup> Oliver Gurney, 'Crashing into the Unknown: An Examination of Crash-Optimization Algorithms Through the Lens of Tort Law' (2013) 5 *Washington Journal of Law, Technology & Arts* 1.

legal protections or obligations. Conversely, individuals harmed by AI systems may struggle to obtain redress due to the absence of defined liability standards.

## **2.5 Cybersecurity Risks and National Security Implications**

AI systems are vulnerable to cybersecurity threats such as data poisoning, adversarial attacks, and model inversion.<sup>19</sup> These threats may compromise the integrity, confidentiality, and availability of AI-driven systems, with significant implications for national security, critical infrastructure, and public safety.

The Cybercrimes Act 2015 provides a general framework for cybersecurity, but it does not address AI-specific vulnerabilities. As Nigeria increasingly adopts AI in sectors such as defence, border control, and public administration, the absence of AI-tailored cybersecurity standards poses substantial risks.<sup>20</sup>

## **3.0 ETHICAL IMPLICATIONS OF ARTIFICIAL INTELLIGENCE IN NIGERIA**

The ethical challenges associated with Artificial Intelligence extend beyond legal compliance and touch on fundamental questions of human autonomy, fairness, transparency, and social justice. As AI systems increasingly shape decision-making in governance, finance, security, and public services, the ethical risks associated with opaque algorithms, biased datasets, and intrusive surveillance become more pronounced. These concerns are amplified in developing societies like Nigeria, where socio-economic inequalities and limited digital literacy heighten

---

<sup>19</sup> Ian Goodfellow and others, 'Explaining and Harnessing Adversarial Examples' (2015) <https://arxiv.org/abs/1412.6572> accessed 12 April 2026.

<sup>20</sup> Luciano Floridi and Josh Cowls, 'A Unified Framework of Five Principles for AI in Society' (2019) 5 *Harvard Data Science Review* 1.

vulnerability to technological harms.<sup>21</sup> Ethical frameworks such as UNESCO's Recommendation on the Ethics of AI emphasise human-centred values, accountability, and fairness—principles that are essential for guiding Nigeria's AI trajectory.<sup>22</sup>

### **3.1 Human Autonomy and the Risk of Technological Overreach**

AI systems increasingly influence decisions that affect individuals' rights, opportunities, and life outcomes. Ethical concerns arise when AI undermines human autonomy by making decisions without meaningful human oversight.<sup>23</sup> In Nigeria, where digital literacy levels vary significantly across socio-economic groups, individuals may be unable to understand or challenge AI-driven decisions, thereby exacerbating power imbalances between technology providers and users.

The ethical principle of human-centred AI emphasises that humans must retain ultimate control over critical decisions, particularly in areas such as healthcare, criminal justice, and public administration.<sup>24</sup> Without clear guidelines on human oversight, AI deployment in Nigeria risks entrenching opaque systems that diminish individual agency and democratic accountability.

### **3.2 Transparency, Explainability, and Public Trust**

Transparency is a core ethical requirement for responsible AI.<sup>25</sup> When AI systems operate without clear explanations, users may lose trust in digital services, particularly in sensitive sectors such as finance, policing, and social welfare. In Nigeria, where public trust in institutions

---

<sup>21</sup> Floridi and Cowls, (n 20)

<sup>22</sup> UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).

<sup>23</sup> Floridi and Cowls (20).

<sup>24</sup> UNESCO (n 22).

<sup>25</sup> OECD, *Principles on Artificial Intelligence* (2019).

is already fragile, opaque AI systems may deepen scepticism and resistance to technological adoption.

Explainability is also essential for ensuring fairness and accountability.<sup>26</sup> For example, if an AI system denies a citizen access to a government benefit, the individual should be able to understand the basis of the decision and challenge it if necessary. Ethical AI frameworks globally emphasise the need for explainable AI (XAI), yet Nigeria lacks statutory or regulatory provisions mandating transparency or explainability in automated systems.

### **3.3 Fairness, Inclusion, and Socio-Economic Equity**

AI systems may inadvertently reinforce existing social inequalities if they are trained on biased or incomplete datasets.<sup>27</sup> In Nigeria, where disparities exist along lines of ethnicity, gender, geography, and socio-economic status, biased AI systems may disproportionately disadvantage marginalised communities.

Ethical AI requires fairness, inclusivity, and representativeness in data collection and model design.<sup>28</sup> However, Nigeria lacks national standards for dataset quality, representativeness, or fairness testing. This gap increases the risk of discriminatory outcomes in areas such as recruitment, credit scoring, and law enforcement.

### **3.4 Labour Displacement and Economic Inequality**

AI-driven automation poses significant ethical and socio-economic challenges, particularly in developing economies.<sup>29</sup> While AI may

---

<sup>26</sup> L. Selbst and J. Powles, 'Meaningful Information and the Right to Explanation' (2017) 7 *International Data Privacy Law* 233.

<sup>27</sup> Barocas and Selbst (n 9).

<sup>28</sup> Jobin, Ienca and Vayena (n 4).

<sup>29</sup> McKinsey Global Institute, *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation* (2017).

create new opportunities in digital sectors, it may also displace workers in manufacturing, agriculture, transportation, and administrative services. Nigeria's labour market, characterised by high unemployment and underemployment, is particularly vulnerable to automation-induced disruptions.

Ethical governance requires proactive strategies to mitigate labour displacement, including reskilling programmes, digital literacy initiatives, and social protection mechanisms.<sup>30</sup> Without such measures, AI adoption may exacerbate inequality and social instability.

### **3.5 Surveillance, Security, and Civil Liberties**

AI-enabled surveillance technologies, such as facial recognition and predictive policing, raise ethical concerns regarding privacy, civil liberties, and state overreach.<sup>31</sup> In Nigeria, where security agencies have broad discretionary powers, the deployment of AI-driven surveillance tools without robust safeguards may lead to abuses, profiling, and violations of constitutional rights.

Ethical AI frameworks emphasise proportionality, necessity, and respect for human rights in the use of surveillance technologies.<sup>32</sup> Nigeria currently lacks statutory oversight mechanisms to regulate AI-enabled surveillance, creating risks of misuse and erosion of civil liberties.

## **4.0 COMPARATIVE PERSPECTIVES ON AI GOVERNANCE**

AI governance models around the world offer valuable insights for Nigeria as it seeks to develop a coherent regulatory framework.

---

<sup>30</sup> World Economic Forum, *The Future of Jobs Report* (2023).

<sup>31</sup> Amnesty International, *Nigeria: Digital Surveillance and Human Rights* (2021).

<sup>32</sup> UN Human Rights Council, *Guiding Principles on Business and Human Rights* (2011).

Jurisdictions such as the European Union, the United States, and the United Kingdom have adopted diverse approaches ranging from comprehensive risk-based regulation to flexible, sector-specific oversight.<sup>33</sup> These global models demonstrate that effective AI governance requires a balance between innovation, human rights protection, and institutional capacity. By examining these comparative frameworks—including the EU AI Act, OECD AI Principles, and UNESCO’s ethical guidelines—Nigeria can identify adaptable strategies that align with its socio-economic realities and regulatory maturity.<sup>34</sup>

#### **4.1 The European Union’s AI Act**

The EU Artificial Intelligence Act (AIA) represents the most comprehensive attempt to regulate AI globally.<sup>35</sup> It adopts a risk-based approach, categorising AI systems into unacceptable, high-risk, limited-risk, and minimal-risk categories. High-risk systems such as those used in healthcare, law enforcement, and critical infrastructure are subject to strict requirements, including transparency, human oversight, data governance, and conformity assessments.

Nigeria can draw valuable lessons from the AIA, particularly regarding risk classification, mandatory impact assessments, and institutional oversight. However, direct transplantation of the EU model may be inappropriate due to contextual differences in institutional capacity, technological maturity, and socio-economic conditions.

---

<sup>33</sup> European Commission, *Artificial Intelligence Act* (2021); White House, *Blueprint for an AI Bill of Rights* (2022); UK Government, *AI Regulation Policy Paper* (2023).

<sup>34</sup> OECD (25).

<sup>35</sup> European Commission, *Artificial Intelligence Act* (2021).

#### **4.2 OECD Principles on Artificial Intelligence**

The OECD Principles on AI emphasise inclusive growth, human-centred values, transparency, robustness, and accountability.<sup>36</sup> These principles have been widely adopted by governments and international organisations. They provide a flexible, non-binding framework that Nigeria can adapt to guide ethical AI deployment while developing its own regulatory architecture.

#### **4.3 UNESCO's Recommendation on the Ethics of AI**

UNESCO's Recommendation on the Ethics of Artificial Intelligence, adopted by 193 member states including Nigeria, provides a global ethical framework grounded in human rights, sustainability, and cultural diversity.<sup>37</sup> It emphasises fairness, transparency, accountability, and environmental responsibility. Nigeria's endorsement of this framework provides a normative foundation for developing national AI governance policies.

#### **4.4 United States and United Kingdom Approaches**

The United States adopts a decentralised, sector-specific approach to AI governance, relying on existing laws and agency-specific guidelines.<sup>38</sup> The United Kingdom, by contrast, promotes a pro-innovation regulatory framework that emphasises flexibility, coordination, and risk-based oversight.<sup>39</sup> These models illustrate alternative pathways for AI governance that Nigeria may consider, particularly in balancing innovation with regulation.

---

<sup>36</sup> OECD (n 5).

<sup>37</sup> UNESCO (n 5).

<sup>38</sup> White House, *Blueprint for an AI Bill of Rights* (2022).

<sup>39</sup> UK Government, *AI Regulation Policy Paper* (2023).

## **5.0 REGULATORY AND INSTITUTIONAL GAPS IN NIGERIA**

Despite growing interest in AI adoption, Nigeria's regulatory environment remains ill-equipped to address the complex challenges posed by autonomous and algorithmic systems. Existing laws such as the NDPA 2023, NITDA Act 2007, and Cybercrimes Act 2015 were not designed with AI in mind and therefore fail to address issues such as algorithmic transparency, automated decision-making, and AI-specific liability.<sup>40</sup> Institutional capacity constraints—including limited technical expertise, weak enforcement mechanisms, and overlapping regulatory mandates—further hinder effective oversight.<sup>41</sup> Addressing these gaps is essential for building a robust, future-ready AI governance framework that protects rights while enabling innovation.

### **5.1 Fragmented Legal Framework**

Nigeria's current legal landscape for AI governance is fragmented across multiple statutes, including the NDPA 2023, the NITDA Act 2007, and the Cybercrimes Act 2015.<sup>42</sup> None of these instruments provides comprehensive regulation of AI, leaving significant gaps in areas such as automated decision-making, algorithmic transparency, liability, and ethical oversight.

### **5.2 Weak Enforcement and Institutional Capacity**

Regulatory agencies such as NITDA, the Nigeria Data Protection Commission (NDPC), and the Nigerian Communications Commission (NCC) face challenges relating to funding, technical expertise, and enforcement capacity.<sup>43</sup> Effective AI governance requires specialised

---

<sup>40</sup> Nigeria Data Protection Act 2023; NITDA Act 2007; Cybercrimes (Prohibition, Prevention, etc.) Act 2015.

<sup>41</sup> NITDA, *Annual Report* (2022).

<sup>42</sup> Nigeria Data Protection Act 2023; NITDA Act 2007; Cybercrimes Act 2015.

<sup>43</sup> NITDA, *Annual Report* (2022).

expertise in machine learning, data science, cybersecurity, and ethics—skills that are currently limited within Nigerian regulatory institutions.

### **5.3 Absence of AI-Specific Legislation**

Nigeria lacks a dedicated AI governance statute. This absence creates uncertainty for developers, investors, and users, and limits the ability of regulators to address emerging risks.<sup>44</sup> A comprehensive AI Act would provide clarity on issues such as liability, transparency, fairness, and human oversight.

### **5.4 Limited Public Awareness and Digital Literacy**

Public understanding of AI technologies remains low in Nigeria, particularly in rural and underserved communities.<sup>45</sup> Without adequate digital literacy, individuals may be unable to exercise their rights, challenge unfair decisions, or engage meaningfully with AI-driven services.

## **6.0 SUMMARY OF FINDINGS**

This article has examined the legal and ethical implications of Artificial Intelligence in Nigeria, highlighting the opportunities and risks associated with AI deployment in a developing digital state. The analysis demonstrates that Nigeria's current regulatory landscape is fragmented, lacking comprehensive AI-specific legislation and institutional capacity to address emerging challenges. Key concerns include data protection gaps, algorithmic bias, opacity in automated decision-making, unclear liability frameworks, cybersecurity vulnerabilities, and ethical issues relating to fairness, transparency, human autonomy, and socio-economic inequality.

---

<sup>44</sup> L Olayemi, 'The Case for an AI Governance Act in Nigeria' (2023) 11 *Nigerian Journal of Technology Law* 77.

<sup>45</sup> National Bureau of Statistics, *Digital Literacy Survey* (2022).

Comparative insights from the European Union, OECD, UNESCO, the United States, and the United Kingdom reveal that Nigeria can draw from global best practices while tailoring its regulatory approach to local socio-economic realities. The study finds that Nigeria requires a coherent, rights-respecting, and context-appropriate AI governance framework that balances innovation with the protection of fundamental rights and societal values.

## **7.0 CONCLUSION**

Artificial Intelligence presents transformative opportunities for Nigeria's socio-economic development, governance efficiency, and global competitiveness. However, without adequate legal and ethical safeguards, AI deployment may exacerbate existing inequalities, undermine civil liberties, and expose individuals and institutions to significant risks. Nigeria's current legal framework anchored in the NDPA 2023, NITDA Act 2007, and Cybercrimes Act 2015 provides a foundational basis for digital governance but remains insufficient for addressing the complex challenges posed by AI.

A comprehensive and forward-looking AI governance framework is essential to ensure that AI technologies are deployed responsibly, transparently, and ethically. Such a framework must incorporate principles of fairness, accountability, human oversight, and respect for fundamental rights. It must also strengthen institutional capacity, promote public awareness, and foster collaboration between government, industry, academia, and civil society.

Nigeria stands at a pivotal moment in its digital transformation journey. The choices made today will shape the trajectory of AI governance for decades to come. A proactive, inclusive, and human-centred regulatory approach will enable Nigeria to harness the benefits of AI while safeguarding the rights and dignity of its citizens.

## **8.0 RECOMMENDATIONS**

The analysis presented in this article demonstrates that Nigeria's current legal and institutional frameworks are insufficient to address the complex challenges posed by Artificial Intelligence. Effective governance requires a proactive, coordinated, and rights-centred approach that balances innovation with the protection of fundamental rights and societal values.<sup>46</sup> Drawing from global best practices and Nigeria's unique socio-economic context, the following recommendations outline the key legal, institutional, and policy reforms necessary to ensure responsible and sustainable AI deployment in the country.<sup>47</sup>

### **8.1 Enact a Comprehensive Artificial Intelligence Governance Act**

Nigeria should develop and enact a dedicated AI Governance Act that addresses key issues such as automated decision-making, algorithmic transparency, liability, fairness, and human oversight. The Act should adopt a risk-based regulatory approach, drawing from the EU AI Act while adapting to Nigeria's socio-economic context.

### **8.2 Establish an Independent Artificial Intelligence Regulatory Authority**

A specialised AI Regulatory Authority should be created to oversee AI deployment, conduct audits, enforce compliance, and develop technical standards. This body should collaborate with existing institutions such as NITDA, NDPC, and NCC while maintaining operational independence.

---

<sup>46</sup> OECD (25).

<sup>47</sup> UNESCO (22).

### **8.3 Mandate Algorithmic Transparency and Explainability**

AI developers and deployers should be required to provide clear explanations for automated decisions, particularly in high-risk sectors such as finance, healthcare, policing, and public administration. Mandatory AI impact assessments should be introduced for high-risk systems.

### **8.4 Strengthen Data Governance and Privacy Protections**

The NDPA 2023 should be expanded to include explicit provisions on automated decision-making, profiling, and algorithmic fairness. Nigeria should also adopt national standards for dataset quality, representativeness, and fairness testing.

### **8.5 Develop AI-Specific Liability Frameworks**

Clear rules should be established to allocate liability among AI developers, manufacturers, operators, and users. This will enhance legal certainty, promote innovation, and ensure effective redress for individuals harmed by AI systems.

### **8.6 Enhance Cybersecurity Standards for AI Systems**

AI-specific cybersecurity guidelines should be developed to address vulnerabilities such as adversarial attacks, data poisoning, and model inversion. Critical sectors should be required to implement robust security measures and conduct regular audits.

### **8.7 Promote Ethical AI Education and Public Awareness**

Government, academia, and civil society should collaborate to promote digital literacy, ethical AI education, and public awareness campaigns. This will empower citizens to understand their rights and engage meaningfully with AI-driven services.

### **8.8 Foster Multi-Stakeholder Collaboration**

Effective AI governance requires collaboration among government agencies, private sector actors, academic institutions, and civil society organisations. Nigeria should establish national AI forums, advisory councils, and public-private partnerships to support responsible innovation.