ISSN: 2579-079X

International Digital Organization for Scientific Research IDOSR JST/26/1220000
IDOSR JOURNAL OF SCIENCE AND TECHNOLOGY 12(2):88-92, 2026.
https://doi.org/10.59298/IDOSR/JST/26/122.8892

Data Privacy and Ethics in AI-Driven Applications in Nigeria: A Review

Mugisha Emmanuel K.

Faculty of Science and Technology Kampala International University Uganda

ABSTRACT

Nigeria's rapid adoption of AI across fintech, telecoms, health, and public services promise faster delivery, wider inclusion, and operational efficiency. Yet the same surge magnifies real-world harms when data practices, model governance, and security controls are weak. This review argues that Nigeria's legal and institutional footing has improved through the Nigeria Data Protection Act (NDPA) 2023 and the establishment of the Nigeria Data Protection Commission (NDPC), but risks persist where "paper compliance" substitutes for end-to-end lifecycle implementation. Key gaps include excessive data collection, opaque data sharing, weak vendor accountability, insecure data/model pipelines, and high-stakes automated decisions with limited transparency or redress. We synthesize safeguards for high-risk deployments credit scoring, biometric identification, clinical decision support, and law-enforcement analytics emphasizing lawful-basis discipline, minimization and retention limits, encryption and access control, documentation of models and datasets, fairness testing, continuous monitoring, and meaningful human oversight with appeal pathways. Finally, we propose a staged, resource-aware roadmap: baseline data mapping and DPIAs, security and contracting hardening, then institutionalized audits, ethics review, and sectoral codes. Trustworthy AI in Nigeria depends on accountable governance, not ambition alone.

Keywords: Nigeria; AI ethics; privacy; NDPA 2023; NDPC; governance; biometric data; fintech; health data; fairness; accountability.

INTRODUCTION

Nigeria's digital economy has evolved into one of Africa's most active innovation ecosystems, driven by rapid mobile-phone penetration, expanding broadband coverage, a vibrant fintech sector, and growing investments in cloud services and data centers. Digital payment platforms, agency banking networks, e-commerce, ride-hailing, logistics, health-tech, and e-government services increasingly rely on data-intensive systems to scale operations, personalize services, and reduce costs [1]. In parallel, national digital identity initiatives and sector-wide digitization (banking, telecommunications, health, education, tax administration, and public safety) are increasing the volume, variety, and velocity of personal and sensitive data generated and processed across the country.

Artificial intelligence (AI) and machine-learning (ML) systems are now embedded within these digital services. In Nigeria, AI-driven applications commonly include fraud detection and anti-money laundering analytics in banking and fintech; automated credit scoring using transactional and alternative data; customer-support chatbots and voice assistants; identity verification and biometric matching for onboarding and authentication; content moderation; predictive maintenance; and clinical decision support such as symptom checkers, triage tools, and diagnostic aids [2]. These systems depend on large datasets transaction logs, call detail records, biometrics, geolocation traces, social media content, device identifiers, and metadata that are often pooled from multiple sources, integrated across platforms, and reused for secondary purposes (e.g., product development, marketing, risk modeling, and behavioral analytics).

While such AI systems can deliver major benefits by improving operational efficiency, reducing fraud losses, widening access to financial services, enhancing service personalization, and enabling faster decision-making, they also raise significant governance challenges. Data-driven automation can amplify privacy harms (e.g., unauthorized disclosure, intrusive profiling, surveillance, re-identification of "anonymized" data), ethical harms (e.g., discrimination, opacity, unfair exclusion from credit or services), and security risks (e.g., data breaches, adversarial attacks, model inversion, prompt injection, and supply-chain compromise through third-party components) [3]. In

high-impact domains like finance, health, and government services, these harms can produce real and lasting consequences: denial of essential services, financial loss, reputational damage, and erosion of trust in digital systems. A Nigeria-focused review is particularly urgent because Nigeria's regulatory environment has matured rapidly in recent years, especially with the enactment of the Nigeria Data Protection Act (NDPA) 2023 and the establishment/strengthening of data protection governance structures yet operational compliance and ethical governance practices often lag behind the speed of AI deployment. Compliance complexity is heightened by Nigeria's socio-technical context: a large informal economy where data capture is fragmented; uneven digital literacy that limits meaningful consent and rights awareness; capacity constraints in enforcement and institutional oversight; and heavy reliance on third-party vendors for cloud hosting, analytics tools, identity services, and outsourced customer operations [4]. These conditions shape distinctive risk drivers, including weak data minimization practices, over-collection, opaque data-sharing arrangements, limited transparency in automated decisions, and inconsistent security baselines across vendors and supply chains. Therefore, understanding how privacy, ethics, and security risks emerge in Nigeria's AI ecosystem and identifying practical governance mechanisms tailored to local realities is essential for building trustworthy AI, protecting individuals, and sustaining growth in the digital economy [5].

Despite the accelerating integration of AI into Nigeria's digital economy, governance systems that should protect individuals and institutions remain uneven and, in many cases, under-implemented. Large-scale collection and processing of sensitive personal data, biometrics for identity verification, location data for service delivery and advertising, financial transaction histories for credit decisions, and communications metadata for fraud analytics often occurs within complex ecosystems involving banks, fintechs, telecom operators, government agencies, data brokers, and cloud/AI vendors. This multi-actor environment creates accountability gaps: it becomes unclear who is responsible when data is misused, when an automated decision is discriminatory, or when a security breach exposes personal information [6]. In practice, organizations may comply with the "form" of regulation (policies, notices, or consent checkboxes) without implementing the "substance" of governance (robust risk assessments, privacy-by-design controls, model transparency, bias evaluation, and continuous security testing). AI systems may be trained or fine-tuned using datasets collected for other purposes, increasing the risk of function creep. Automated credit scoring and fraud detection tools may embed or reproduce societal inequalities if the training data reflects historical bias or if proxy variables (location, device type, spending patterns) correlate with protected attributes. Meanwhile, the cybersecurity attack surface is expanding: centralized data repositories and APIs, cloud misconfigurations, insider threats, weak identity and access management, and AI-specific threats (e.g., prompt injection in chatbots, data poisoning, model extraction) can all compromise confidentiality, integrity, and system reliability [7]. Although Nigeria now has stronger legal foundations for data protection, there remains a need to systematically examine how AI deployments interact with privacy, ethics, and security risks in the Nigerian context, and to identify governance strategies that are feasible for institutions operating under resource constraints and high vendor dependence. Without such evidence-based guidance, Nigeria risks escalating public distrust, regulatory non-compliance, harms to vulnerable populations, and setbacks to digital inclusion [8]. This study seeks to review and synthesize evidence on the privacy, ethical, and security risks associated with AI-driven applications within Nigeria's fast-expanding digital economy, while identifying governance and compliance strategies that fit local realities and align with Nigeria's evolving data protection framework. In practical terms, it will map dominant AI use-cases across key sectors and the kinds of data they rely on, trace how risks emerge along the AI lifecycle (collection, processing, sharing, modeling, deployment, and monitoring), and assess gaps between what regulation requires and what institutions actually implement. The study is significant in four main ways. First, it has strong policy relevance: by consolidating where AI risks are most acute and where compliance commonly fails, it can support regulators and policymakers in refining guidance, prioritizing enforcement, developing sector-specific codes of practice, and strengthening capacity-building toward measurable protections rather than "paper compliance." Second, it advances institutional governance and risk management for banks, fintechs, telecoms, health-tech firms, and public agencies by translating evidence into actionable controls privacy-by-design, data minimization, lawful basis and consent management, vendor and third-party risk controls, security baselines, model governance, documentation, incident response, and audits of automated decision systems. Third, it strengthens protection of individuals and digital inclusion by foregrounding fairness, transparency, accountability, and user rights, particularly for low-income and digitally vulnerable groups who may face disproportionate harm from opaque AI decisions. Finally, it contributes academically and practically by filling a Nigeria-specific evidence gap, guiding future empirical research, and providing a baseline for comparison with peer African digital economies and for tracking progress over time. Overall, the study aims to build trust by aligning AI innovation with enforceable privacy, ethical safeguards, and resilient security practices.

Methods

This article adopts a narrative review design to synthesize multidisciplinary evidence on AI, privacy, and governance in Nigeria. Evidence is drawn primarily from Nigerian legal and regulatory materials, notably the Nigeria Data Protection Act (NDPA, 2023) and interpretive guidance issued by the Nigeria Data Protection Commission (NDPC).

To capture practical compliance realities, the review also considers sector-specific rules and supervisory expectations across high-impact domains such as financial services, telecommunications, and health, where personal data processing and automated decision-making are increasingly embedded in service delivery. These normative sources are complemented by relevant policy documents and peer-reviewed scholarship on AI ethics, privacy engineering, and algorithmic governance, with particular attention to concepts and tools that translate to low-resource settings (e.g., proportionate risk controls, privacy-by-design, and feasible accountability mechanisms). The synthesis is structured around five linked components: (i) Nigeria's evolving regulatory framework; (ii) illustrative sectoral use-cases and deployment contexts; (iii) a risk taxonomy spanning legal, technical, and socio-institutional risks; (iv) mitigation strategies and governance models for responsible AI and data protection; and (v) a Nigeria-specific implementation roadmap that aligns compliance, capacity building, and oversight with local institutional constraints and opportunities.

Nigeria's Data Protection and Institutional Landscape

Nigeria has transitioned from a largely "soft-law" data protection era under the Nigeria Data Protection Regulation (NDPR) 2019 to a clearer statutory framework with the Nigeria Data Protection Act (NDPA) 2023. The NDPA established the Nigeria Data Protection Commission (NDPC) and vested it with oversight and enforcement authority, improving legal certainty for personal data processing, stronger data subject rights, security obligations, cross-border transfer rules, and organizational accountability duties [9]. For AI deployments, Nigeria's framework aligns with core global principles that are especially operational: lawfulness, fairness, and transparency (including explainability and non-deceptive processing); purpose limitation to prevent "mission creep," particularly with biometric and public-sector datasets; data minimization and proportionality to avoid collecting unnecessary sensitive attributes; accuracy through data quality controls and ongoing model performance monitoring; storage limitation via retention schedules and deletion; and integrity and confidentiality through security safeguards and breach readiness. Accountability is central, requiring documentation, governance structures, vendor controls, and data protection impact assessments. In practice, AI projects face pressure points around choosing lawful bases beyond consent where power imbalances exist, handling sensitive data (health, biometrics, children's and location data), managing automated decision-making in credit or eligibility contexts, ensuring compliant cross-border transfers for cloud and offshore analytics, and tightening vendor/processor governance across outsourced development and SaaS ecosystems [10].

AI Use-Cases in Nigeria and Their Risk Profiles

AI deployment in Nigeria spans high-impact sectors with distinct but overlapping risk profiles. In fintech and credit scoring, AI powers fraud detection, anomaly tracking, AML alerts, BNPL risk models, and automated support; yet proxy variables (e.g., device type, geolocation, network metadata) can encode socio-economic or ethnicity-linked bias, while opaque models undermine explanation and appeal rights. Aggressive data harvesting contacts, SMS logs, expansive device permissions and reuse of KYC data beyond original purposes heighten privacy and function-creep concerns [11]. In telecoms and adtech, churn prediction, targeted ads, and network optimization rely on granular behavioral and mobility data, raising risks of location profiling, sensitive-trait inference, opaque third-party sharing, weak consent granularity, and re-identification from "anonymized" datasets. Digital health tools triage bots, diagnostic aids, and claims automation processes highly sensitive data, exposing patients to leakage, biased recommendations, poor validation, unclear liability, and secondary data use without robust governance. Public-sector AI in biometrics, eligibility scoring, and surveillance risks exclusion errors, disproportionate harms to vulnerable groups, limited redress, and politicization [12]. In security contexts, facial recognition and predictive policing amplify false positives, discrimination, civil-liberty chilling effects, and weak oversight absent rigorous impact assessments.

Ethics Frameworks Applicable to the Nigerian Context

Ethical guidance for AI typically converges on beneficence, non-maleficence, autonomy, justice, and explicability, but in Nigeria these principles must be applied through local realities that shape how harm occurs and who bears it. Structural inequality raises the risk that AI systems deepen exclusion from credit, healthcare, and public services, especially when datasets overrepresent urban populations [13]. Digital literacy disparities complicate meaningful consent: people may accept terms they cannot interpret, and may lack practical routes to access, correct, or delete data. Power asymmetries citizen versus state, consumer versus platform, worker versus employer can also weaken voluntariness and amplify surveillance, coercion, or retaliation. Infrastructure constraints, including uneven cybersecurity maturity and limited incident response capacity, further elevate exposure to breaches and misuse [14]. A Nigeria-ready ethical framework should therefore prioritize contestability (clear appeals and remedies), human oversight for high-stakes decisions, auditability across the AI lifecycle, and targeted harm reduction for vulnerable groups, rather than relying on abstract transparency alone. In parallel, risk taxonomy should cover privacy threats (re-identification, inference attacks, model leakage, breach exposure, and over-retention) and societal harms (bias, opacity, automation bias, exclusion of languages/regions, and accountability gaps across controllers, processors, and vendors) [15].

Practical Mitigation Strategies

Practical mitigation of AI privacy and ethics risks starts with privacy-by-design. Systems should minimize data by collecting only necessary features and prohibiting contact-list or SMS scraping unless strictly required and lawful. Purpose limitation must be enforced through dataset "use contracts," tagging, and access controls tied to defined purposes. Core security controls include encryption in transit and at rest, secrets management, MFA, logging, and key rotation. De-identification should be treated as risk reduction, not elimination, with re-identification testing. Where feasible, federated learning or on-device processing can reduce central data pooling, while differential privacy can harden analytics and training pipelines in telecom and adtech [16]. Ethical governance should require DPIAs/AI impact assessments for high-risk uses (biometrics, credit, health), plus model documentation (datasheets, model cards, decision logs), fairness testing across geography, gender (where lawful), and language groups, and explainability with contestability via appeals and human review. Vendor and cross-border governance need strong DPAs, transfer risk assessments, and "no shadow datasets" clauses. Sectorally: fintech must ensure explainable, auditable scoring; health needs local validation and clinician accountability; public biometrics demands proportionality, oversight, and published impact assessments [17].

Roadmap for Nigeria

Nigeria's privacy-and-AI compliance roadmap can be staged for speed, depth, and long-term ecosystem impact. In the first 0–6 months, organizations should lock in baseline compliance and quick wins by mapping all personal-data flows end-to-end, clarifying controller vs processor responsibilities, and publishing practical retention schedules that reduce over-collection and storage risk. In parallel, they should roll out DPIA templates for high-risk processing and apply minimum security controls (access management, encryption where appropriate, logging, and vendor due diligence). Consent and transparency must be upgraded fast: clearer notices, layered privacy information that is easy to scan, and support for local languages to improve meaningful user understanding. Over 6–18 months, the focus shifts to mature AI governance, standardizing model documentation, fairness and bias testing, monitoring, and repeatable audit routines, while building robust incident response through breach drills and tabletop exercises [18]. An ethics review board should be established for high-risk AI, bringing legal, security, product, and domain experts together. Beyond 18 months, Nigeria can strengthen the ecosystem via sectoral codes of practice, certification schemes, harmonized procurement standards, independent audits for sensitive systems, transparency reporting, and NDPC-led capacity building with universities and industry on privacy engineering and AI safety.

CONCLUSION

Nigeria's AI surge across fintech, telecoms, health, and public services can accelerate inclusion and efficiency, but it also amplifies real-world harms when data practices, model governance, and security controls are weak. This review shows that the NDPA 2023 and the NDPC have strengthened Nigeria's legal and institutional foundation, yet "paper compliance" without lifecycle implementation leaves persistent gaps over-collection, opaque data sharing, weak vendor accountability, insecure pipelines, and high-stakes automated decisions with limited transparency and redress. High-risk use cases credit scoring, biometric ID, clinical decision support, and law-enforcement analytics require proportionate safeguards: lawful basis discipline, data minimization, retention limits, encryption and access control, documented models and datasets, fairness testing, continuous monitoring, and human oversight with clear appeal pathways. A staged roadmap is feasible even under resource constraints: establish baseline data mapping and DPIAs, harden security and contracts, then institutionalize audits, ethics review, and sector codes. Trustworthy AI in Nigeria will be built through accountable governance, not ambition alone.

REFERENCES

1. Iddrisu, K., Alhassan, F., Giamporcaro, S., Abor, J.Y.: The Rise of FinTech in Africa: Empowering the Underserved and Unbanked. Presented at the October 1 (2025)
2. Odufisan, O.I., Abhulimen, O.V., Ogunti, E.O.: Harnessing artificial intelligence and machine learning for fraud detection and prevention in Nigeria. J. Econ. Criminol. 7, 100127 (2025). https://doi.org/10.1016/j.jeconc.2025.100127
3. Aldasoro, I., Gambacorta, L., Korinek, A., Shreeti, V., Stein, M.: Intelligent financial system: How AI is transforming finance. J. Financ. Stab. 81, 101472 (2025). https://doi.org/10.1016/j.jfs.2025.101472
4. C1P1T: Safeguarding the New Oil: A Spotlight on Nigeria Data Protection Act 2023, https://cipit.strathmore.edu/safeguarding-the-new-oil-a-spotlight-on-nigeria-data-protection-act-2023/, (2023)
5. Alum, E.U., Ugwu, O.PC. Artificial intelligence in personalized medicine: transforming diagnosis and treatment. *Discov Appl Sci* **7**, 193 (2025). https://doi.org/10.1007/s42452-025-06625-x
6. Parambil, M.M.A., Rustamov, J., Ahmed, S.G., Rustamov, Z., Awad, A.I., Zaki, N., Alnajjar, F.: Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. Comput. Educ. Artif. Intell. 7, 100327 (2024). https://doi.org/10.1016/j.caeai.2024.100327

7.von Grafenstein, M., Jakobi, T., Stevens, G.: Effective data protection by design through interdisciplinary research methods: The example of *effective* purpose specification by applying user-Centred UX-design methods. Comput. Law Secur. Rev. 46, 105722 (2022). https://doi.org/10.1016/j.clsr.2022.105722

8.Echegu D. A., Artificial Intelligence (AI) in Customer Service: Revolutionising Support and Engagement. IAA Journal of Scientific Research 11(2):33-39, 2024. https://doi.org/10.59298/IAAJSR/2024/112.3339

9.International Transfers of Health Data: A Global Perspective 9789819799824, 9789819799831, https://dokumen.pub/international-transfers-of-health-data-a-global-perspective-9789819799824-9789819799831.html

10. Oduro, S., Moss, E., Metcalf, J.: Obligations to assess: Recent trends in AI accountability regulations. Patterns. 3, 100608 (2022). https://doi.org/10.1016/j.patter.2022.100608

11. Ezeonwumelu, J. O. C., Uhama, K. C., Ugwu, O. P. C., Alum, E. U., Ugwuanyi, A. C., Tambwe, P. R. (2024). The Impact of Artificial Intelligence and Machine Learning on Pharmacy Practice. Research Invention Journal of Research in Medical Sciences 3(1):10-15.

12. Which Campaigns Benefit Most from C+DV? Prospecting, Reach/Traffic, and Retention by the Numbers, https://www.northbeam.io/blog/which-campaigns-benefit-most-from-c-dv-clicks-deterministic-views

13. Luis A B, Pablo R (2023). The application of artificial intelligence-based tools to intralingualrespeaking: The NER Buddy. *Proceedings of the International Workshop on Interpreting Technologies SAY IT AGAIN 2023: 2-3 November/Malaga, Spain. 9-15.*

14. Epstein, D., Quinn, K.: Markers of Online Privacy Marginalization: Empirical Examination of Socioeconomic Disparities in Social Media Privacy Attitudes, Literacy, and Behavior. Soc. Media Soc. 6, 2056305120916853 (2020). https://doi.org/10.1177/2056305120916853

15. Abujaber, A.A., Nashwan, A.J.: Ethical framework for artificial intelligence in healthcare research: A path to integrity. World J. Methodol. 14, 94071 (2024). https://doi.org/10.5662/wjm.v14.i3.94071

16. George U A, Kolawole A O, Ebenezer E (2023). Critical review on the application of artificial intelligence techniques in the production of geopolymer-concrete. *SN Applied Sciences, 5, (8), 217.*

17. Abhishek, A., Erickson, L., Bandopadhyay, T.: Data and AI governance: Promoting equity, ethics, and fairness in large language models. MIT Sci. Policy Rev. (2025). https://doi.org/10.38105/spr.cb0t0jkorb

18. Long, S.A.L.-W.R., Blythe, F., Cuyvers, L., Bruynseraede, M.: Privacy, Data Protection and Cybersecurity: EU Overview, https://www.lexology.com/library/detail.aspx?g=937f0564-6deb-441a-bd8d-f04b2beaac9b

CITE AS: Mugisha Emmanuel K. (2026). Data Privacy and Ethics in AI-Driven Applications in Nigeria: A Review. IDOSR JOURNAL OF SCIENCE AND TECHNOLOGY 12(2):88-92, 2026. https://doi.org/10.59298/IDOSR/JST/26/122.8892