F.A. GARRICK & CO
LEGAL PRACTITIONERS, PATENT, TRADEMARK AND DESIGN LAW AGENTS

JANUARY 2026

Data Privacy and Artificial Intelligence: Legal Implications and Regulatory Direction

www.fagarrickco.com

Introduction

Artificial intelligence is no longer a developing or experimental tool, it has become part of everyday decision-making across finance, employment, telecommunications, public administration, and digital commerce, with credit assessments, recruitment processes, content moderation, targeted advertising, and even public-sector functions increasingly relying on automated systems, all of which are connected by their reliance on personal data.

As Artificial Intelligence systems become more deeply embedded in economic and social life, questions about how personal data is collected, analysed, inferred, and used have become unavoidable, and these questions are not merely technical but legal in nature, because although modern data protection laws were not drafted with complex machine-learning models in mind, data privacy law now provides the primary framework through which Artificial Intelligence systems are regulated where personal data is involved, making it necessary to examine how existing data privacy rules apply to artificial intelligence, the risks that arise from Artificial Intelligence-driven data processing, and the direction of regulatory oversight.

Artificial Intelligence as Personal Data Processing

From a legal perspective, artificial intelligence is not regulated because it is autonomous or intelligent but because it processes personal data, and both the EU General Data Protection Regulation (GDPR)[1] and Nigeria's Data Protection Act 2023 (NDPA)[2] adopt deliberately broad definitions of "processing" that cover any operation performed on personal data, whether automated or manual.

Artificial Intelligence (AI) systems clearly fall within this definition[3] as they collect data directly from individuals, draw from third-party

[1] EU General Data Protection Regulation, Regulation (EU) 2016/679, OJ L 119/1, 4 May 2016, arts 4(2), 5, 6, 13–15, 22, and 35.
[2] Section(s) 2, 24, 25, 26, 30, and 34 Nigeria Data protection Act 2023
[3] European Data Protection Board, Guidelines 3/2019 on Processing of Personal Data through Video Devices adopted on the 29th January 2020(as revised), and Guidelines 05/2020 on Consent under Regulation 2016/679, relevant for secondary use and purpose limitation in AI training.

sources, analyse large datasets, and generate predictions or classifications relating to identifiable persons, and importantly, AI systems do more than process existing data because they frequently create new personal data through inference, for example by predicting behaviour, preferences, creditworthiness, or risk profiles, outputs that often have real consequences for individuals and must therefore be treated as personal data for legal purposes.

Nigerian courts have already made it clear that liability in this area depends on the act of processing itself rather than the sophistication of the technology involved, as seen in ***Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission***[4], where the Federal High Court held that the collection and handling of personal data without proper legal safeguards amounted to a breach of privacy rights[5] even where the processing was carried out in pursuit of public objectives, reinforcing a straightforward principle that once personal data is processed, the obligations imposed by data protection law apply regardless of whether the processing is carried out by humans or algorithms.

Core Data Protection Principles and AI

One of the most difficult issues raised by Artificial Intelligence (AI) is its compatibility with basic data protection principles, particularly lawfulness, fairness, and transparency, since data protection laws require organisations to identify a lawful basis for processing personal data and to ensure that such processing is fair to the data subject, yet in practice many AI systems operate in ways that are difficult to explain even to their developers[6], leaving individuals unaware that AI is being used at all or unable to understand how decisions affecting them are made.

Purpose limitation and data minimisation present further challenges because AI systems are often trained on large datasets originally collected for entirely different purposes, raising legitimate legal questions about whether using existing data for AI training is compatible with the purpose for which that data was first obtained, and where consent is relied upon, organisations must be able to show that it was properly informed and sufficiently specific to cover AI-driven processing[7].

Accuracy is another area of concern as AI systems frequently produce probabilistic outputs rather than factual conclusions, yet these predictions can influence decisions about employment, credit, insurance, or access to essential services, while data protection law requires personal data to be accurate and kept up to date, a requirement that becomes more complex when applied to inferred or predictive information.

Nigerian case law supports the enforcement of these principles, as illustrated in ***Godfrey Nya Eneye v MTN Nigeria Communications Ltd***[8], where the Federal High Court found that the unauthorised handling of a subscriber's personal data constituted a violation of privacy rights, and although the case did not involve artificial intelligence, it confirms unfair data practices will

[4] Incorporated Trustees of Digital Rights Lawyers Initiative v National Identity Management Commission (Unreported, Federal High Court, Abuja Judicial Division, Suit No FHC/ABJ/CS/815/2020).
[5] Section 37 of the Constitution of the Federal Republic of Nigeria, 1999 as amended
[6] UK Information Commissioner's Office, Explaining Decisions Made with AI (2020), paras 2.1–2.5.
[7] European Data Protection Board, Guidelines 3/2019 on Processing of Personal Data through Video Devices adopted on the 29th January 2020(as revised)
[8] Godfrey Nya Eneye v MTN Nigeria Communications Ltd (2019) LPELR-47442(CA).

attract legal consequences even in technologically mediated environments, reasoning that applies equally to AI-driven processing.

Automated Decision-Making and Profiling

The most legally sensitive aspect of AI deployment arises where decisions are made automatically, with the GDPR's Article 22[9] providing individuals with the right not to be subject to decisions based solely on automated processing where such decisions produce legal or similarly significant effects, protections that are mirrored under Nigeria's Data Protection Act 2023.

These rules do not prohibit automated decision-making outright but instead impose safeguards, such that where automated decisions are permitted, organisations must ensure meaningful human involvement, allow individuals to express their views, and provide mechanisms for challenging decisions.

Regulatory enforcement in Nigeria reflects increasing attention to automated and large-scale data processing, with the Nigeria Data Protection Commission (NDPC)[10] exercising its powers to impose sanctions for failures relating to transparency, consent, and improper processing, and although enforcement actions have not yet focused explicitly on artificial intelligence, they demonstrate a clear regulatory position that automated processing affecting individuals must be explainable, accountable, and capable of justification, with responsibility remaining with the data controller even where decisions are produced by algorithms or outsourced systems.

Bias, Discrimination, and Fairness

Artificial Intelligence (AI) systems inevitably reflect the data on which they are trained, and where datasets contain historical bias or structural inequality, AI systems may reproduce or even amplify discriminatory outcomes[11], and while data protection law is not a substitute for anti-discrimination legislation, it provides important tools for addressing unfair or unlawful processing[12].

Principles of fairness, accuracy, and restrictions on profiling can be used to challenge AI systems that systematically disadvantage particular groups, concerns that also intersect with Nigeria's constitutional framework, as Section 42[13] guarantees freedom from discrimination while data protection law reinforces fairness and accountability in the handling of personal data, allowing data privacy law to operate as an early legal safeguard against algorithmic practices that undermine equality and human dignity.

Cross-Border Data Processing and Jurisdiction

AI systems often rely on global infrastructure and cross-border data flows, with personal data collected in one jurisdiction, processed in another, and stored elsewhere, and both the General Data Protection Regulation (GDPR) and the Nigeria Data Protection Act (NDPA) impose

[9] General Data Protection Regulation, Regulation (EU) 2016/679
[10] Nigeria Data Protection Commission (NDPC), Guidance Notice on Registration of Data Controllers and Data Processors of Major Importance (2024) and NDPC Enforcement Notices 2023–2024.
[11] Section 42 Constitution of the Federal Republic of Nigeria 1999 as amended
[12] OECD, Principles on Artificial Intelligence (OECD Legal Instrument, 2019)https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
[13] Constitution of the Federal Republic of Nigeria 1999 as amended

strict conditions on cross-border transfers that require organisations to ensure transferred data receives an adequate level of protection.

Nigerian regulators have shown a willingness to assert jurisdiction over foreign technology companies whose practices affect Nigerian residents, as demonstrated in ***Federal Competition and Consumer Protection Commission v Meta Platforms Inc & WhatsApp LLC***[14], where significant penalties were imposed for violations relating to data privacy and consumer protection, underscoring the point that reliance on foreign servers or multinational vendors does not shield organisations from Nigerian regulatory oversight where Nigerian personal data is involved.

Regulatory Direction and the Future of AI Governance

Globally, regulators are beginning to supplement data protection law with Artificial Intelligence-specific rules, with the EU Artificial Intelligence Act[15] adopting a risk-based approach that imposes additional obligations on high-risk AI systems, particularly those affecting fundamental rights.

Nigeria does not yet have AI-specific legislation, but the NDPA[16] already provides a workable framework for regulating AI-driven personal data processing, and as AI adoption increases across sectors such as finance, telecommunications, and public administration, regulatory scrutiny is likely to intensify.

Conclusion

Artificial intelligence presents clear benefits but also reshapes how personal data is used and controlled, and where personal data is involved, data privacy law remains the primary legal framework governing AI deployment, making transparency, fairness, accountability, and human oversight legal obligations rather than aspirational standards.

Organisations that deploy AI systems must therefore treat privacy as a core governance issue rather than a post-deployment concern, since integrating data protection considerations into the design and operation of AI systems is essential both to manage legal risk and to support the development of responsible and trustworthy technology.

[14] Federal Competition and Consumer Protection Commission v Meta Platforms Inc & WhatsApp LLC (FCCPC Final Order and Penalty Decision, 2023).
[15] European Union Artificial Intelligence Act Regulation (EU) 2024/1689
[16] Nigeria Data Protection Act 2023

FOR MORE INFORMATION, PLEASE CONTACT:

Nosa John Graham Garrick
Senior Partner
nosa.garrick@fagarrickco.com

Bola Osineye
Managing Partner
bola.osineye@fagarrickco.com

F.A. GARRICK & CO

LEGAL PRACTITIONERS, PATENT,
TRADEMARK AND DESIGN LAW AGENTS

Corporate Office:
45 Calutta Cres, Apapa Quays, Lagos

Phones:
Nosa John Graham Garrick: +234 811 215 9999
Bola Osineye:+234 808 644 3239

Emails:
Info@fgarrickco.com
Nosa.garrick@fgarrickco.com
Bola.osineye@fgarrickco.com

Website: www.fagarrickco.com