

ARTIFICIAL INTELLIGENCE LIABILITY AND THE LAW: LEGAL RESPONSIBILITY FOR AI DRIVEN DECISIONS IN NIGERIA



By Record Of Law / February 20, 2026

Authored By: Kefas Deborah Kaura

Nasarawa State University Keffi Nasarawa State

ABSTRACT

The increasing deployment of artificial intelligence (AI) systems in decision making processes across financial, administrative, commercial and virtually all sectors has introduced complex questions of legal responsibility. In Nigeria, AI technologies are now routinely used in Credit Scoring, Recruitment processes, Surveillance, fin-tech services, Human Resource Management, research and Data analytics, yet the law remains largely silent on liability for harm caused by AI driven decisions. This article examines whether existing Nigerian legal principles are sufficient to address liability arising from AI related harm. It analyses tortious, contractual, consumer protection, and data protection frameworks, highlighting doctrinal gaps in fault, causation, and accountability where autonomous or semi-autonomous systems are involved both in the private and public sector. Drawing comparative insights from the European Union and the United Kingdom, the article argues that Nigeria should adopt a structured and forward-looking approach to AI liability that preserves innovation while ensuring accountability and access to justice.

INTRODUCTION

Artificial intelligence has moved from theoretical discourse into practical application, transforming how decisions are made across modern societies. In Nigeria, AI enabled systems increasingly influence outcomes in Banking, Telecommunications, Digital Governance, Security Surveillance, and Employment Processes. While these technologies promise efficiency and objectivity, they also create significant legal challenges when their decisions result in harm.

Traditional legal frameworks are premised on human agency, intention, and control. Liability doctrines in tort and contract assume that wrongdoing can be traced to a human actor capable of foresight and restraint. Artificial Intelligence disrupts this assumption by introducing systems capable of learning, adapting, and producing outcomes that are not entirely predictable by their designers or operators. When AI denies a loan, discriminates in recruitment, or misidentifies a citizen in a surveillance database, the question of responsibility becomes blurred. The absence of clear answers creates what legal Scholars have described as a “responsibility gap”, where harm occurs without a readily identifiable legal wrongdoer .

Beyond private-sector applications, AI is increasingly being explored by the Nigerian government in public administration, digital identification, and security systems. These applications bring efficiency but also increase the risk of systemic harm where AI decisions are flawed. The potential impact extends beyond individuals to constitutional rights and public trust, making AI liability a critical public law concern.

LEGAL FRAMEWORK AND LITERATURE REVIEW

Nigeria currently lacks legislation specifically regulating artificial intelligence. Existing legal regimes such as tort law, contract law, consumer protection, and data protection therefore provide the primary avenues for addressing AI-related harm. However, these regimes were developed to determine liability with human decision making in mind and are often not suited to autonomous systems.

WHO BEARS RESPONSIBILITY? KEY PARTIES IN AI LIABILITY

Determining fault in AI errs involves multiple actors. Here is a breakdown relevant to Nigerian scenarios:

Developers and Manufacturers: Often the primary targets. If an AI algorithm is poorly designed (e.g. trained on biased data reflecting Nigeria’s diverse ethnicities), developers could be liable under negligence. Globally, cases like Uber’s 2018 self-driving car fatality held the company accountable; in Nigeria, similar logic applies via tort law.

Deployers and Operators: Businesses integrating AI, such as a Lagos fintech using chatbots for customer service. If the AI errs (e.g., giving wrong financial advice), the company is vicariously liable for its “agent.”

Users and End-Consumers: In some cases, misuse by users (e.g., overriding AI safety features in a drone) shifts blame. However, if the AI is marketed as foolproof, strict liability protects consumers.

ARTIFICIAL INTELLIGENCE AND GENERAL LEGAL LIABILITY

Literature on AI and liability highlights the inadequacy of fault-based models for autonomous systems. Because AI can operate independently of direct human input, insisting on proof of human fault may allow organizations to evade accountability. This concern is especially significant in Nigeria, where victims often lack the technical resources needed to challenge complex algorithmic decisions. Some scholars advocate for liability frameworks that allocate risk to entities deploying AI rather than focusing solely on individual fault.

Beyond data protection, general principles from tort, contract and consumer protection laws fill the void:

Tort Law (Negligence and Nuisance): Rooted in common law, as seen in cases like *Donoghue v. Stevenson*, which influences Nigerian jurisprudence, liability arises if someone owes a duty of care, breaches it, and causes harm. For AI, if a developer fails to test an algorithm adequately, leading to errors, that could be negligent. Nigerian courts have applied this in product liability cases, such as defective goods causing injury.

Negligence remains the cornerstone of civil liability in Nigerian law, requiring proof of duty of care, breach, causation, and damage. Applying these elements to AI-driven harm raises conceptual and evidentiary difficulties, particularly in relation to causation and foreseeability. The lack of certainty as it pertains legal liability of machine-learning systems complicates the claimant’s burden of proof and challenges traditional judicial reasoning.

In the context of AI related harm, the existence of a duty of care may be relatively straightforward. Organizations that deploy AI systems in high risk context such as Banks, Employers and government agencies, can reasonably be said to owe duties to affected individuals . however, proving breach is considerably more difficult where harm arises from algorithmic behaviour rather than direct human error.

Causation presents even a greater challenge. Nigerian Courts traditionally require a direct and clear causal link between breach and damage. The complexity and opacity of machine learning systems make it practically impossible for claimants to demonstrate how a particular decision resulted from a specific failure. This places victims at a structural and disadvantage and risk denying effective remedies.

Foresee-ability is another challenge. While organizations may anticipate general risks associated with AI deployment, predicting specific harmful outcomes is often impossible. Courts that strictly require foresee-ability may leave victims without remedy. One approach is to treat the mere decision to deploy a high-risk AI system as creating foreseeable risk, enabling liability even if the exact harm was not predictable.

Contract Law: If AI is part of a service agreement, breaches can lead to claims. For instance, a Nigerian bank using AI for loan approvals must ensure it doesn't violate contractual terms of fairness. The law in Nigeria recognizes electronic evidence, aiding proofs in AI-related disputes.

Product Liability: Under the Consumer Protection Council Act and standards from the Standards Organisation of Nigeria (SON), AI embedded products (like smart devices) are treated as goods. If defective, manufacturers are strictly liable, meaning no need to prove negligence, just that the product caused harm. This echoes global trends but is under-tested in AI contexts here.

Intellectual Property and Other Laws: The Copyright Act 2022 and Patents and Designs Act touch on AI-generated works, but ownership remains unclear, potentially complicating liability if AI "creates" infringing content.

VICARIOUS LIABILITY AND ORGANIZATIONAL RESPONSIBILITY

One possible response to the accountability gap created by artificial intelligence is the extension of vicarious liability principles to AI systems. Under this approach, organizations would be held responsible for harm caused by AI systems deployed in the course of their business. While this aligns with policy considerations of risk allocation and victim protection, it stretches traditional doctrine, as AI is neither an employee nor an agent in the conventional sense.

Nonetheless, Nigerian courts have previously demonstrated flexibility in adapting legal principles to changing social and economic realities. A similar approach may be required to ensure that the deployment of AI does not undermine access to justice or legal accountability.

This approach aligns with the principle of enterprise liability, which holds entities benefiting from risky activities accountable for resulting harm. Nigerian courts have previously adapted legal principles to ensure fairness and deterrence, suggesting that extending liability to AI systems is doctrinal feasible and socially justified.

CONTRACTUAL AND CONSUMER PROTECTION LIABILITY

AI systems increasingly perform contractual functions. Where harm arises, liability may be framed as breach of contract. However, exclusion clauses in standard form agreements often limit remedies. Consumer protection law offers some safeguards, but it does not expressly regulate algorithmic decision making.

AI systems increasingly perform contractual functions, including automated contracting, risk assessment, and service delivery. Where AI malfunction results in loss, liability may arise from breach of express or implied contractual terms, particularly obligations relating to fitness for purpose and reasonable care.

However, many technology driven contracts are standard-form agreements containing exclusion or limitation clauses. Nigerian courts generally uphold such

clauses unless they are unconscionable or contrary to public policy. This creates a risk that consumers may be left without effective remedies for AI-induced harm.

Information asymmetry between AI providers and users further complicates liability. Consumers and corporate clients often cannot fully understand the risks or mechanics of AI systems, which weakens the protective function of contract law. Without regulatory intervention, contractual risk allocation may consistently favour providers, leaving harmed parties without effective remedies.

DATA PROTECTION AND REGULATORY LIABILITY

The Nigeria Data Protection Act 2023 is particularly relevant to AI systems that rely on personal data. Although the Act does not explicitly regulate AI, its provisions on lawful and fair processing may apply to automated decision-making that infringes data subject rights.

Automated decision-making may produce discriminatory or unlawful outcomes, especially where biased datasets are used. While the Act does not expressly regulate artificial intelligence, its provisions on lawful, fair, and transparent processing can be interpreted to apply to AI-driven decision-making systems.

AI systems may also replicate social biases present in historical data, producing discriminatory outcomes. Data protection law partially addresses these harms, but it does not prevent broader societal consequences such as systemic inequality or exclusion. This underscores the need for AI specific regulatory mechanisms in addition to data protection.

COMPARATIVE PERSPECTIVE

The European Union has adopted a structured approach through the proposed Artificial Intelligence Act and AI Liability Directive, while the United Kingdom relies on a principles based model. These approaches offer valuable lessons for Nigeria, particularly in easing the burden of proof for victims.

Lessons from the European Union and United Kingdom demonstrate the importance of proactive regulation. Nigeria may initially lack capacity for fully comprehensive AI laws, but adopting clear principles on accountability, transparency, and risk management would provide immediate guidance and reduce liability gaps.

CHALLENGES IN ENFORCING AI LIABILITY IN NIGERIA

Attribution of Fault: AI's opacity makes proving causation difficult. Who "caused" an error; the code, the data, or external factors.

Jurisdictional Issues: With global AI firms like Google operating here, enforcing judgments across borders is tricky, though treaties like the Hague Convention help.

Regulatory Gaps: No mandatory AI audits or risk assessments, unlike the EU. This leaves victims relying on slow court processes.

Internationally, the EU AI Act 2021 imposes high-risk AI requirements, including transparency and human oversight, with fines up to €35 million. The US focuses on sector-specific rules, while Africa's landscape varies; South Africa and Egypt lead with strategies. Nigeria could adopt a hybrid: a national AI policy incorporating global best practices.

FINDINGS AND OBSERVATIONS

This article finds that Nigerian law currently lacks a coherent framework for AI liability and that reliance on traditional doctrines alone is insufficient to ensure accountability.

These observations indicate that AI liability is both a doctrinal and structural issue. Without legal reform, the growing reliance on AI risks creating areas of accountability, undermining both technological adoption and public confidence in the legal system.

CONCLUSION AND RECOMMENDATIONS

In conclusion, artificial intelligence is no longer a distant concept in Nigeria; in fact, it represents both the present and the future of the global community, one in which Nigeria is certainly not left behind. It is already shaping how Nigerians work, trade and interact. Yet, as we embrace the benefits of AI, we must also prepare for its legal and ethical implications. Ensuring accountability when algorithms err is essential to maintaining public trust and safeguarding rights in our digital age.

Nigeria must adopt a forward-looking yet context-sensitive approach to AI regulation. Legislative reform, judicial capacity building, and regulatory guidance are essential to ensure that innovation does not outpace accountability.

Innovation without accountability risks eroding public trust and undermining fundamental rights. As artificial intelligence becomes more deeply embedded in Nigerian society, the absence of a clear liability framework may discourage responsible deployment and deny effective remedies to victims of AI-related harm.

The regulation of AI requires balancing innovation and accountability. Overly restrictive laws could stifle technological progress, while inadequate regulation risks systemic harm.

Nigeria's legal system, grounded in established principles and capable of evolution, is well-positioned to develop a context-sensitive framework for AI accountability.

Before the enactments of these laws as recommended above, Nigerians can do the following based on category;

For Businesses: Conduct AI impact assessments, include indemnity clauses in contracts, and comply with the Nigerian Data Protection Act 2023. Also train staff on AI use management and risks.

For Individuals: Read and understand the terms of service for AI tools, analyze its effect through the objective test and report errors to regulators like the Nigeria Data Protection Commission, and seek legal advice promptly.

For Policymakers: Enact an AI Act focusing on liability, drawing from the European Union Artificial Intelligence Act 2021 while suiting our context, emphasizing affordability for startups, the private sector, organisation, and general applicability

REFERENCE(S):

Nigerian Data Protection Act, 2023

European Commission, Artificial Intelligence Act (2021).

Abbott R, 'The Reasonable Computer: Disrupting the Paradigm of Tort Liability' (2018) 86 George Washington Law Review 1.

Burrows A, 'A Restatement of the English Law of Contract' (OUP 2016).

OECD, 'Artificial Intelligence and Liability' (2019).

Pagallo U, 'The Laws of Robots: Crimes, Contracts, and Torts' (Springer 2013).