RETHINKING LEGAL RESPONSIBILITY IN THE AI ERA: BALANCING COMPENSATION, BLAME, AND DETERRENCE.

Esther Adeyemi[1]

University of Lagos || estheradeyemi2002@gmail.com

[1] Esther Adeyemi || University of Lagos || estheradeyemi2002@gmail.com

Abstract:

As AI becomes increasingly prevalent, questions surrounding legal responsibility for AI-related harm persist. This article examines emerging liability theories, including strict liability, negligence, and product liability, through real-world scenarios like autonomous vehicle accidents and medical device malfunctions. The article argues for a multifaceted approach to AI liability, combining elements of each theory to ensure accountability, prevent harm, and promote innovation. Using a mixed-methods approach, the research draws on a comprehensive literature review, landmark cases, and national and international AI policies.

Keywords: Artificial Intelligence, Liability, Accountability, Negligence, Product Liability.

1.0 INTRODUCTION

Artificial Intelligence (AI), coined by computer scientist John McCarthy in 1956, has evolved from science fiction to reality, transforming industries and redefining human interaction. The concept of AI dates back to the 1950 Dartmouth Summer Research Project on Artificial Intelligence, where McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon explored the possibilities of machine intelligence.[2] The first AI program, Logical Theorist, was developed in 1956 by Allen Newell and Herbert Simon. This pioneering program was designed to simulate human problem-solving abilities. Since then, AI has progressed rapidly, with significant milestones including the first AI-powered robot, Shakey, developed at Stanford Research Institute (SRI) in 1969. From 1980 - 1990, expert systems and rule-based AI emerged, and machine learning and neural networks also gained prominence. By 2011, IBM's Watson defeated human champions in jeopardy.[3]

However, AI's growth has not been without incident. One notable example is the 1971 ELIZA chatbot experiment,[4] where users became emotionally attached to the AI, highlighting potential risks and unforeseen consequences. More recent incidents underscore the need for accountability, in 2017, the wannaCry ransomware attack exploited AI-powered vulnerabilities not just that, in 2018, Uber's autonomous vehicle killed a pedestrian in Tempe, Arizona and in the same year, Google's AI-driven breast cancer detection showed promise, but raised concerns about bias and accountability.

Today, AI's global market value is projected to surpass $15 trillion by 2028, with 83% of organisations leveraging AI for innovation and efficiency[5]. Autonomous vehicles navigate public roads, AI-powered chatbots revolutionise customer service, and predictive analytics inform medical diagnoses. Yet, this rapid growth raises critical questions about accountability. As AI assumes greater autonomy, traditional notions of liability, data protection, and intellectual property are severely tested. Self-learning algorithms, opaque decision-making processes, and autonomous actions blur accountability lines. The consequences are far-reaching, impacting human rights, social justice, and societal fabric.

2.0 WHEN AI FAILS: AREAS WHERE LEGAL RESPONSIBILITY COMES INTO PLAY

"Ubi jus ibi remedium" - Where there is a right, there is a remedy. This ancient legal maxim underscores the fundamental principle of legal responsibility, ensuring individuals and entities are held accountable for their actions. The Nigerian courts have held severally that “the maxim is so fundamental to the administration of justice that where there is no remedy provided by common

[2] Russell, Stuart J. and Peter Norvig Artificial Intelligence: A Modern Approach (3rd end, Prentice Hall 2010)
[3] 'IBM- Watson Defeats Humans in Jeopardy' CBS News 17 February 2011
[4] Oshan Jarow from ELIZA onwards, humans love their digital reflections " available at https://www.vox.com/future-perfect/23617185/ai-chatbots-eliza-chatgpt-bing-sydney-artificial-intelligence-history"(accessed 5 March 2023)
[5] Grand View Research. (2022). Artificial Intelligence Market Size, Share & Trends Analysis.

law or statutes, the courts have been urged to create one.[6] The court cannot therefore be deterred by the novelty of an action." [7] However, Artificial Intelligence (AI) disrupts this notion, sparking intense debate about traditional liability frameworks.

Firstly, AI's integration into contract law raises concerns about autonomous breaches. For instance, AI systems can generate electronic signatures, but their validity remains uncertain. Moreover, AI may enter into contracts without human oversight, potentially leading to unintended obligations. In *SEC v Knight Capital America's LLC*[8], an AI-powered trading system malfunctioned, causing Knight Capital Group to lose $440 million in 45 minutes. This incident raises questions about AI's capacity to execute contracts and its liability for breaches.

Meanwhile, tort law faces challenges in attributing fault to AI systems, algorithmic fault, negligence, causation, and damages assessment. In 2018, an Uber self-driving car struck and killed Elaine Herzberg, raising concerns about AI's liability in tort law.[9] This case underscores the complexities of attributing fault to AI systems. In *Cruz v Raymond Talmadge*[10], involved a common AI-driven product a GPS device. The plaintiffs were injured, some critically when a bus in which they were riding struck an overpass. At the time of the accident, the bus driver was using two GPS devices manufactured by different companies. The plaintiffs brought claims against those GPS manufacturers based on traditional theories of negligence, breach of warranty and strict liability, they also based their claims on traditional product liability principles. Similarly, in *Hills v Fans Robotics America, Inc.,*[11] The plaintiff brought suit in connection with injuries caused by workplace robots. The plaintiff sued his employer, the grocery store, claiming that it was vicariously liable because one of the store's managers disabled the malfunctioning safety light curtain and instructed employees to place the robot on hold rather than stooping the robot entirely if needed to approach it. Those actions allegedly violated standard operating policies for the robot, safety light curtain and automated palletization system. The jury held that the employers were 65% responsible, and the designers of the automated palletization system were 25% responsible for the plaintiff's injuries.

In addition, AI-facilitated cyber-attacks pose significant threats to criminal law, and malicious AI enables more sophisticated hacking techniques, making accountability difficult. In *United States v. Park Jin Hyok*[12], the WannaCry ransomware attack, facilitated by AI-powered malware, affected 200,000 computers worldwide. This incident highlights AI's role in exacerbating cyber threats. Through AI, individuals' facial data has been used to create pornographic imagery, while others

[6] "Liability for Damage caused by Artificial Intelligence" Templars 11 November 2021
[7] See Bello v. A.-G., Oyo State (1986) 5 NWLR (Pt. 45) 828 Orianzi v. A.-G., Rivers State (2017) 6 NWLR (pt. 1561)224
[8] No. 2:12-cv-06760, 2012
[9] Amrita Vasudevan, "Addressing the Liability Gap in AI Accidents" (2023) Policy Brief No. 177
[10] United States District Court District of Massachusetts Civil Action No.)15-13258-NMG
[11] No. 2:2004cv02659 - Document 180 (E.D. La. 2010)
[12] No. 2:18-mj-01479, (C.D. Cal.)

have had their voices replicated to trick family and close friends over the phone often, to send money to a scammer.[13] For instance, in the *Charlotte child psychiatrist case, where a 40-year-old child psychiatrist used AI to generate pornographic images with children's pictures.*[14] *The court held him liable for 40 years in prison for sexual exploitation of a minor and using Artificial intelligence to create pornography images.*

Furthermore, AI-generated creative works raise intellectual property concerns thus, authorship, originality, and fair use defences require clarification. The AI-generated painting sold at Christie's auction sparks debates about AI authorship.[15] This incident challenges traditional notions of intellectual property. Furthermore, the case of *Alter v. Open AI*[16]Highlights copyright infringement concerns, as AI-generated content raises questions about ownership and authorship.

Another significant challenge is, AI's role in healthcare necessitates stricter regulations to prevent fatal errors. AI-powered medical devices and algorithms have been said could cause harm if flawed or biased. As far back as the 1980s, Therac-25, a radiation therapy machine developed by Atomic Energy of Canada Limited"AECL"[17] Delivered damaging doses of radiation to cancer patients due to a glitch in the complex coding, with fatal results, liability, in this case, is still debated today as some hospitals have their upgrades to the systems that arguably cause overdose.

AI's automation capabilities also threaten jobs and economic stability. According to McKinsey, up to 800 million jobs could be lost worldwide by 2030. Automation replaces human workers in sectors like manufacturing, customer service, and transportation. Self-service kiosks and automated retail systems have already replaced human cashiers. AI's environmental impact raises concerns also because training AI models requires massive computational resources, which contributes to e-waste generation and resource exploitation.

Cyber threats are another significant concern. AI systems can be compromised, leading to financial loss, data theft, and reputational damage. Additionally, malicious AI can lead to the spread of malware, conduct phishing attacks, and disrupt critical infrastructure. In 2024, hackers breached NIMC's database, exposing sensitive information of over 200,000 Nigerians, including National Identity Numbers (NIN), addresses, and dates of birth.[18] This leads to the exposure of citizens' personal data to be compromised, potentially leading to identity theft and fraud. The NIMC

[13] "Criminals are using AI in terrifying ways — and it's only going to get worse" New York Post 10 May 2023
[14] "Horribly Twisted Charlotte pornography case shows the 'unsettling' reach of AI-generated imagery" FBI 29 April 2024
[15] "AI Art at Christie's Sells for $432,500" The New York Times, 25 October 2018
[16] No. 1:23-cv-10211, (S.D.N.Y.)21 Nov 2023
[17] Charles Huff. 2003. A History of the Introduction and Shut Down of Therac-25. Online Ethics Center. DOI:. available at https://onlineethics.org/cases/therac-25/history-introduction-and-shut-down-therac-25.
[18] Justice Okamgba "NIMC facing multiple unauthorised accesses to NIN data – Stakeholders" available at https://punchng.com/nimc-facing-multiple-unauthorised-accesses-to-nin-data-stakeholders/(accessed 25 June 2024)

acknowledged the breach, assured citizens that necessary measures were being taken to secure the database, and urged citizens to report suspicious activities.

AI systems often require vast amounts of personal data, and these systems infringe on individual rights. This brings privacy violations leading to identity theft, stalking, and reputational damage. The integration of Artificial Intelligence (AI) in surveillance systems raises alarming concerns about privacy. AI-powered monitoring can track individuals' movements, analyze online behaviour, and collect personal data. Governments and corporations exploit AI-driven surveillance, compromising individual rights. Facial recognition technology, smart home devices, and social media platforms collect sensitive information, often without consent. AI's insatiable data hunger fuels invasive surveillance, eroding trust and autonomy. In 2020, the Nigerian Immigration Service (NIS) Biometric Data Breach brought criticism to the NIS for allegedly compromising the biometric data of millions of Nigerians through its AI-powered database.[19] Furthermore, In *FTC v. Facebook, Inc,*[20] Facebook faced a $5 billion fine for allowing Cambridge Analytical to harvest user data without consent. This case illustrates AI's capacity to facilitate data breaches and the need for enhanced privacy protections.

The opacity of the AI decision-making process often referred to as the black box problem complicates efforts to trace accountability back to a specific entity.[21]. Artificial Intelligence's (AI) lack of transparency and explainability erodes trust and accountability. "Black box" decision-making processes obscure AI's reasoning, hindering error identification, bias detection, and accountability. Consequences include: unfair outcomes, discrimination, and inadequate oversight. For instance, Google's AI-powered search results were said to lack transparency.

AI can be used for social manipulation. AI-generated content can spread false information. Influence campaigns and these AI-powered bots can manipulate public opinion. This can erode trust in institutions. For example, AI-powered bots have been used to spread political disinformation[22] also Chat GPT accusing a professor of sexual harassment[23].

Despite the challenges posed by Artificial Intelligence (AI), its numerous benefits cannot be overlooked. AI enhances efficiency, accuracy, and innovation, transforming industries and improving lives. Its advantages include automated processes, data analysis, predictive insights, and

[19] ITEdge News Nigeria Immigration Service publishes uncollected passport details, breaches data privacy law" available at https://www.itedgenews.africa/nigeria-immigration-service-publishes-uncollected-passport-details-breaches-data-privacy-law/(accessed 7 October 2024)
[20] No. 1:2020cv03590 - Document 90 (D.D.C. 2022)
[21] Cheng, Varshney and Liu, 2021 Li,et,al.2023
[22] Nick Hajli "Election disinformation: how AI-powered bots work and how you can protect yourself from their influence" available at https://theconversation.com/election-disinformation-how-ai-powered-bots-work-and-how-you-can-protect-yourself-from-their-influence-227174 (accessed 9 April 2024)
[23] Jason Nelson "ChatGPT Wrongly Accuses Law Professor of Sexual Assault" available at https://decrypt.co/125712/chatgpt-wrongly-accuses-law-professor-sexual-assault (accessed 7 April 2023)

personalized experiences, ultimately driving economic growth, scientific progress, and social advancements, underscoring the importance of harnessing AI's potential.

3.0 THE AI ACCOUNTABILITY CONUNDRUM: CHALLENGES AND COMPLEXITIES

The emergence of Artificial Intelligence (AI) has revolutionized various sectors, raising complex questions about legal responsibility. The allocation of liability for AI-driven harm necessitates reevaluation, considering factors like development process, deployment context, user interaction, continuous learning, and adaptation. The dynamic nature of AI, enabled by advanced machine learning techniques, makes it challenging for developers to predict system modifications, control future behavior, and anticipate potential risks.

When machines cause damage, yet cannot be held responsible, who should bear the liability? Intuitively, one might point to the AI developer, after all, when traditional hardware like a hair dryer malfunctions, we typically hold the manufacturer accountable. However, AI systems differ significantly from conventional machines, complicating the assignment of responsibility to developers. According to Nissenbaum, there are four barriers to accountability: the problem of many hands, “bugs” in the system, the computer as a scapegoat, and ownership without liability. The problem of too many hands relates to the fact that many groups of people (programmers, engineers, etc.) at various levels of a company are typically involved in the creation of a computer program and have input into the final product. When something goes wrong, there is no one individual who can be held responsible.[24]

Furthermore, advanced machine learning techniques, such as facial recognition in CCTV cameras, enable AI to learn, adapt, and evolve over time. This dynamic nature makes it challenging for developers to predict how the system will modify itself, control its future behaviour and anticipate potential risks. Advanced machine learning techniques create unpredictability, raising questions about liability allocation, developers' liability for unforeseen consequences and responsibility shifting to users or operators are pressing concerns.

These questions have fueled debates among legal scholars, with some jurisdictions exploring the concept of strict liability, holding entities responsible for the outcome of AI systems they deploy irrespective of fault. Strict liability principles, as in *Rylands v. Fletcher*, [25]may apply holding entities responsible for AI outcomes irrespective of fault. A no-fault liability system where compensation is provided without the need to prove negligence is also being considered to streamline the accountability process. In 1985, the EU Product Liability Directive (henceforth, ``PLD''), established a strict liability regime where producers are liable for their defective products regardless of

[24] Nissenbaum, Helen, “Computing and Accountability, “Communications of the ACM, 37:1, p. 73 (1994). available at http://delivery.acm.org/10.1145/180000/175228/p72nissenbaum.pdf?ip=128.62.211.38&id=175228&acc=ACTIVE%20SERVICE&key=

[25] (1866) L.R.1. Exch. 265, affirmed (1868) L.R. 3 H.L. 330.

whether the defect is their fault.[26] The PLD assigns liability to the ``producer'' (Article1 PLD), which includes the manufacturer of a finished product, the producer of any raw material or the manufacturer of a part, and any person who, by putting his name, trademark or other distinguishing feature on the product presents himself as to its producer.[27] Apart from the European Union, countries like Singapore,[28] Canada,[29] California, USA[30]. Strict liability however may stifle innovation, as developers and manufacturers may be deterred by potential liability. Imposing strict liability for damages caused by inherently uncontrollable AI devices raises fairness concerns like would innovators dare develop or utilize these products under such conditions? Strict liability's application to AI may lead to excessive liability where developers and manufacturers may face crippling financial burdens, stifling innovation and hindering AI's potential benefits. Conversely, inadequate liability may fail to provide sufficient recourse for harmed individuals. The 2018 Uber self-driving car accident in Tempe, Arizona, illustrates the complexities of strict liability in AI. The National Highway Traffic Safety Administration (NHTSA) investigation revealed a combination of human error, software flaws, and inadequate testing contributed to the fatal crash. Allocating liability among Uber, the software developers, and the vehicle manufacturer proved contentious advancement.

Product liability, focusing on defective AI products or software, protects consumers and encourages quality control but struggles to define "defect" and address AI's complex nature. Under German law, it has been argued that AI liability should come under the concept of product liability. However, it is somewhat difficult to consider AI as a product due to its tendency to make autonomous decisions. Negligence, a fundamental tort law principle, requires demonstrating a breach of duty, causation, and harm. In AI contexts, negligence can arise from various scenarios, including design or manufacturing defects, inadequate testing or quality control, insufficient training data, and failure to update or maintain AI systems. However, negligence faces challenges in AI-related cases, such as defining duty and breach, causation, and foreseeability. Despite these challenges, negligence remains a vital framework for addressing AI-related harm. Courts must consider factors such as industry standards and best practices, reasonable foreseeability of harm, and expert testimony on AI design and functionality. For instance, in cases involving AI-powered medical devices, courts may consider industry guidelines for device testing and maintenance.

Vicarious liability, another critical tort law principle, holds employers or principals responsible for harm caused by employees or agents. In AI contexts, vicarious liability can arise from employer-

[26] Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products [1985] OJ L 210/29 (Product Liability Directive). Given that liability is restricted to defective products, some argue that this is in fact a fault-based liability regime. See e.g. Herbert Zech, 'Liability for AI: public policy considerations' (2021) 22 ERA Forum 147
[27] Article3(2) PLD.
[28] Singapore Government, "Artificial Intelligence Governance Framework" (2019)
[29] Government of Canada, "Bill C-27" (2022)
[30] California State Legislature, "Assembly Bill 2189" (2020)

employee relationships, principal-agent relationships, and independent contractor relationships. However, vicarious liability faces unique challenges in AI-related cases, such as autonomy, control, and attribution.

Actus non facit reum nisi mens sit rea" (An act does not make a person guilty unless the mind is guilty) emphasizing the importance of intent, or mens rea, which complicates criminal liability attribution. Traditional criminal law relies on intent, knowledge, or recklessness to establish guilt. *Section 36 (12)* of the Constitution of the Federal Republic of Nigeria states that 'a person shall not be convicted of an offence unless that offence is defined and the penalty therefore is prescribed in a written law'. The next is Sections 28 and 30 of the Criminal Code which exempts from criminal liability persons who the law deems to lack the mental capability (doli incapaxi) of committing an offence whether because of tender age or insanity. Section 30 exempts from criminal responsibility for any act or omission all persons under the age of 7 years, and also persons under the age of 12 years for any act or omission, unless it is proved that at the time of doing the act or making the omission he could know that he ought not to do the act or make the omission. Section 28 is to the effect that one is not criminally responsible for an act or omission if at the time of doing the act or making the omission the person is in such a state of mental disease or natural mental infirmity as to deprive him of capacity to understand what he is doing or of capacity to control his actions, or of capacity to know that he ought not to do the act or make the omission.[31] Once one element is missing, no criminal liability can be imposed. In Nigeria, as with most parts of the world, a crime is said to be committed when a person recognized as such by the law and who is not statutorily excluded from being criminally culpable, does an act or makes an omission defined by the statutes to be an offence, and such a person did such an act or made such an omission with the required criminal knowledge or intent. When this happens, a crime can be said to have been committed. [32] Many machine learning systems exhibit 'black box' characteristics, making it challenging or impossible for humans, including developers and application servers, to comprehend their decision-making processes. This opacity raises critical questions about accountability. Thus, the doctrine of "*Qui facit per alium facit per se*" (He who acts through another, acts himself) plays a crucial role in attributing legal responsibility for Artificial Intelligence (AI) actions. This doctrine holds principals liable for actions performed by their agents or intermediaries, including AI systems. In the context of AI, this doctrine faces challenges and offers advantages. The challenges in applying "*Qui facit per alium facit per se*" to AI arise from AI's autonomy and complexity. AI's independent decision-making complicates determining whether the principal truly controls the AI's actions. Moreover, AI's intricate programming and data processing make it difficult to establish clear lines of authority. This uncertainty hinders accountability for AI-related harm. Despite these challenges, applying "Qui facit per alium facit per

[31] ORAEGBUNAM & UGURU: "Artificial Intelligence Entities And Criminal Liability: A Nigerian Jurisprudential Diagnosis" AFJCLJ 3 (2018)
[32] ibid

se" to AI offers significant advantages. Holding principals liable promotes responsible AI development and deployment, serving as a deterrent against reckless AI deployment. This approach also ensures consistency with existing agency law principles.

Furthermore, what happens when the developer is no longer existent (e.g., bankrupt or dissolved)? Developer insolvency poses a significant challenge in attributing legal responsibility for Artificial Intelligence (AI). When developers become bankrupt or dissolved, victims of AI-related harm face substantial obstacles in seeking redress, leading to a void in accountability. The consequences of developer insolvency are far-reaching. Victims are left without a viable defendant to pursue claims against, resulting in uncompensated harm. Moreover, insolvent developers escape accountability, undermining deterrent effects. This lack of recourse not only harms individuals but also erodes trust in AI technology. Pursuing claims against insolvent developers is fraught with challenges. Identifying successors or assigns of the original developer is difficult, and asset tracing is complex. Jurisdictional issues further complicate cross-border claims, highlighting the need for harmonized regulatory frameworks.

The attribution of legal responsibility for AI-related damages is crucial but insufficient to compensate victims adequately or prevent harm effectively. Ultimately, a comprehensive regulatory framework must account for AI's complexities and evolving nature.

4.0 AI REGULATION IN NIGERIA: A REVIEW OF EXISTING LAWS, REGULATORY, FRAMEWORK, AND ENFORCEMENT MECHANISM

This chapter delves into the intricacies of existing laws, policies, and regulations governing AI, both domestically and internationally. Artificial Intelligence (AI) has gradually become an integral part of Nigeria's technological landscape. The country's journey with AI began in the early 2000s, with the establishment of the National Information Technology Development Agency (NITDA). NITDA's primary objective was to promote and regulate the use of information technology in Nigeria.

However, before diving into the provisions of NITDA, it is important to begin with the Constitution. As the grundnorm of the Federal Republic of Nigeria, the 1999 Constitution (as amended) provides the foundation for the country's legal framework. The Constitution's provisions serve as the bedrock for all laws governing Artificial Intelligence (AI) in Nigeria. Specifically, Section 4(1) provides that the legislative powers of the Federal Republic of Nigeria shall be vested in a National Assembly for the Federation, which shall consist of a Senate and a House of Representatives." Section 4(2)(b)"The National Assembly shall have power to make laws for the peace, order and good government of the Federation concerning any matter included in the Exclusive Legislative List. "The Exclusive Legislative List is contained in Part I of the Second Schedule to the Constitution and includes matters such as National security, Foreign policy, Aviation, Telecommunications, Copyright, Patents, and Trademarks.

Additionally, Section 4(4) allows the National Assembly to make laws for the Federation on any matter not included in the Exclusive Legislative List, provided it is not inconsistent with any law enacted by the National Assembly. This provision empowers the National Assembly to enact laws related to Artificial Intelligence (AI), such as Data Protection, Cyber security, Intellectual property, and Consumer protection enabling the regulation of AI in Nigeria.

The 1999 Constitution of the Federal Republic of Nigeria (as amended) provides the foundation for Nigeria's legal framework on AI. Section 14(2)(b) of the Constitution guarantees the right to freedom from discrimination, which is crucial in ensuring AI systems do not perpetuate biases., Section 39 protects the right to freedom of expression, encompassing the development and deployment of AI-generated content. Furthermore, Section 44(1) safeguards the right to privacy, essential in regulating AI-driven data collection and processing.

The Constitution indirectly protects intellectual property through Section 39, which guarantees freedom of expression. This section implies protection for creative works, including literary, musical, and artistic creations. Section 44(1) of the Constitution, which safeguards the right to acquire and own property, also extends to intellectual property. This provision ensures that individuals can own and protect their intellectual creations. The right to privacy, enshrined in Section 37 of the Constitution, serves as the bedrock for data protection. This section protects individuals' right to private and family life, which necessarily encompasses the protection of personal data. Furthermore, Section 39, guaranteeing freedom of expression, implies the right to control personal information.

The Constitution addresses health through Section 17(3)(d), which imposes an obligation on the State to provide adequate medical facilities. This provision recognizes the importance of healthcare and empowers the government to prioritize public health. Section 45(1) of the Constitution further reinforces this commitment, granting the State the authority to make laws for public health. This provision enables the government to enact legislation addressing health concerns, such as the National Health Act, of 2014. While the 1999 Constitution does not explicitly address data protection, health, and intellectual property, its provisions lay the groundwork for safeguarding these rights. Supplemental laws and regulations have filled the gaps, ensuring Nigeria's legal framework adequately protects these critical interests. While AI-specific legislation is still in development, existing laws provide a foundation for regulating AI.

To counter cyber threats, Nigeria enacted the Cybercrimes (Prohibition and Prevention) Act of 2015, which provides a comprehensive blueprint for addressing these issues. In 2020, the National Information Technology Development Agency (NITDA) rolled out guidelines that have direct and indirect implications for various aspects of AI utilization in Nigeria. [33] The Cybercrimes

[33] Josephine Uba Artificial intelligence (AI) Goes wrong: Real life cases and Regulatory Implications of the Negative Effects of AI in Nigeria available at https://oal.law/artificial-intelligence-ai-goes-wrong/

(Prohibition, Prevention, etc.) Act, 2015 is a pivotal legislation regulating AI-driven cyber threats. Section 2 prohibits unauthorized access to computer systems, including AI-powered networks, while Section 3 criminalizes cyber threats, including AI-driven attacks. Furthermore, Section 5 mandates data authentication and integrity, crucial for AI systems. Section 12 establishes penalties for cybercrime offences, including AI-related incidents, demonstrating the Act's significance in regulating AI.

The Nigeria Data Protection Act, 2022 (repealing Data Protection Regulation, 2019) is another critical legislation. Section 2 defines personal data, encompassing AI-processed information. Section 3 mandates data protection by design and default, applicable to AI systems. Section 15 regulates automated decision-making, including AI-driven profiling, ensuring transparency and accountability.

In the financial sector, the Security and Exchange Commission (SEC) Rules on Robo-Advisory Services, 2018 provide guidance. Rule 1 defines Robo-Advisory Services, including AI-powered investment advice. Rule 3 mandates registration and licensing for Robo-Advisory Services, ensuring regulatory oversight. The Federal Competition and Consumer Protection Act, of 2018 also addresses AI. Section 123 prohibits unfair business practices, including AI-driven deceptive marketing. Section 125 mandates transparency in consumer contracts, applicable to AI-driven services. Section 130 establishes consumer protection agencies to address AI-related complaints. Intellectual property rights are protected under the Copyright Act, 2022. Section 2 defines copyrightable works, including AI-generated content. Section 5 regulates copyright infringement, applicable to AI-driven piracy. Section 6 establishes the rights of authors, including AI-generated works.

Lastly, the Nigerian Communication Commission Act, of 2003 empowers the NCC to regulate telecommunications, including AI-powered services (Section 70). Section 75 mandates licensees to ensure network security, relevant to AI-driven networks. Nigeria's AI landscape is thriving, with a vibrant pan-African ecosystem driven by private entities, businesses, and startups at the forefront of implementing and evolving AI systems. The country's data protection regulation, NDPR, aligns with international standards, safeguarding individual data privacy and ensuring secure transactions involving personal data exchange.[34]This regulation is similar to the European Union's General Data Protection Regulation.

Globally, organizations like the United Nations are playing a crucial role in shaping AI governance. This initiative includes UNESCO's Recommendation on the Ethics of Artificial Intelligence. This provides a framework for ethical AI development and deployment. The European Union's General

[34] ibid para 12

Data Protection Regulation (GDPR) sets standards for data protection and AI-driven decision-making.

Although Nigeria currently lacks a formalized national AI policy, NITDA, in collaboration with NCAIR and other stakeholders, is driving progress through numerous government ministries, departments, and organizations. This partnership aims to promote responsible AI development and deployment. These efforts demonstrate Nigeria's commitment to developing a robust AI ecosystem that prioritizes security, privacy, and responsible innovation.

In conclusion, Nigeria's regulatory framework for AI is evolving, with existing laws addressing critical aspects such as cyber security, data protection, consumer protection, intellectual property, and telecommunications. While these laws do not directly address AI, they provide a foundation for regulating AI's impact on Nigerian society.

V. Recommendations and Solutions for Attributing Legal Responsibility to AI

Existing liability frameworks, rooted in human intent, are ill-equipped to address AI-driven harm. The autonomy, learning capacity, and interconnectedness of AI systems require adapting traditional models of accountability. A risk-based approach offers a balanced solution by allocating responsibility according to the level of control and risk involved in AI deployment. Developers, deployers, and users should therefore bear corresponding degrees of liability based on their influence over AI outcomes. Developing AI-specific insurance and compensation mechanisms can further ensure accountability and victim protection. Products such as cyber, product liability, and error-and-omission insurance cover AI-specific risks, while compensation funds and AI harm remediation processes guarantee redress. Mandatory AI insurance, coupled with regulatory standards, would provide financial security and clarity in cases of AI-related harm.

The complexity of AI development also calls for shared liability. Since AI-related harm often arises from the interaction of users, manufacturers, and designers, shared responsibility ensures comprehensive redress and fosters collaboration. It encourages responsible innovation while safeguarding human welfare. Effective shared liability frameworks must clearly define stakeholder roles, proportionate liability, and continuous adaptation to emerging risks.

Another innovative idea is recognizing AI as a legal person, similar to corporations. Legal personhood would acknowledge AI’s capacity to act, enter contracts, and be held accountable. Historically, corporations have been granted legal personality to bear rights and obligations; similarly, “electronic personhood” could be extended to advanced AI systems. Under such a model, AI entities would be registered, and their human controller’s developers or owners would remain ultimately liable. This approach promotes accountability, clarifies legal standing, and encourages safer AI design. The European Parliament and Law Commission of England and Wales have already considered such frameworks, showing growing international consensus.

Awareness and education are equally essential. Dispelling myths of AI infallibility helps individuals and organizations understand its biases, vulnerabilities, and limitations. Educational programs can promote AI literacy, critical thinking, and policy understanding empowering the public and lawmakers to make informed decisions about AI governance.

Finally, the establishment of regulatory bodies is vital for oversight and standard-setting. Independent agencies with technical expertise can develop and enforce design, testing, and deployment standards, investigate incidents, and ensure transparency. Institutions like the European Commission's AI Regulatory Body and the U.S. Federal Trade Commission's AI Task Force exemplify proactive regulation. Global cooperation is also necessary to harmonize AI laws, ensuring consistency, innovation, and accountability across borders. In sum, achieving accountability in the age of artificial intelligence requires a multifaceted approach: risk-based and shared liability, AI-specific insurance, possible legal personhood, public education, and robust regulation. Together, these measures can foster a trustworthy AI ecosystem that prioritizes safety, responsibility, and human well-being.

V. Conclusion

As AI continues to advance, our legal frameworks must adapt, prioritizing flexibility and responsiveness to emerging challenges, policymakers, developers, and stakeholders must collaborate to establish comprehensive AI governance, ensuring accountability and societal alignment. Ultimately, attributing legal responsibility to AI requires striking a balance between technological innovation and human judgment, ensuring that AI serves humanity's best interests. By reimagining liability frameworks and embracing regulatory oversight, we can unlock AI's full potential, fostering a future where technology enhances human life without compromising accountability.