ARTIFICIAL INTELLIGENCE AND CORPORATE CRIMINALITY: EMERGING CHALLENGES IN LIABILITY AND ACCOUNTABILITY

Shajobi-Ibikunle Gloria* and Shajobi Oseghale Deborah Oluwadamilola**

Abstract

Traditional liability doctrines such as vicarious liability, the identification doctrine, and organisational fault, struggle to accommodate AI-driven decisions, particularly where autonomous systems act without direct human involvement. This article examines the emerging challenges of corporate criminal liability in the age of artificial intelligence (AI). It explored how AI is deployed as both a tool and a potential perpetrator of corporate misconduct, ranging from algorithmic trading and collusion to money laundering and cybercrime. The article adopted a doctrinal methodology drawing on primary and secondary sources of Law in Nigerian, as well as other jurisdictions. The article found that while AI itself cannot bear criminal responsibility, corporations must remain accountable for the risks created by its deployment. The article recommends reforms, including stricter compliance obligations, hybrid liability models, and harmonisation of international regulatory standards. In addition, regulatory frameworks must increasingly emphasise the role of corporate governance structures, compliance programmes, whistleblowing mechanisms, and independent algorithmic audits as essential safeguards against the risks posed by AI deployment and misuse. The paper concludes that effective governance of AI within corporate contexts will depend on striking an appropriate balance between fostering innovation and ensuring accountability.

Keywords: Artificial Intelligence, Corporate Criminal Liability, Organisational Fault, Algorithmic Collusion, Cybercrime, Corporate Governance.

1.0 Introduction

Corporate criminality has long since posed significant challenges to regulators, courts, and policymakers. Traditionally, such crimes involve fraudulent accounting, insider trading, money laundering, or environmental offences committed through a corporation's structures. However, with the rapid integration of artificial intelligence (AI) into corporate operations, ranging from algorithmic trading and automated compliance systems to decision-making in supply chain management, the question of corporate liability for AI-driven misconduct has become increasingly urgent[1].

The integration of artificial intelligence (AI) into corporate operations presents unprecedented challenges for corporate criminal liability. Traditionally, corporate misconduct such as fraud, market manipulation, or money laundering has been addressed through doctrines of vicarious liability, identification, and organisational fault[2]. However, these frameworks struggle to accommodate autonomous decision-making by AI systems, particularly where no human mind can be identified. Unlike traditional human actors, AI systems operate autonomously, often with limited or no direct human oversight. This raises a profound legal dilemma: who should bear criminal responsibility when AI facilitates or directly engages in conduct that would otherwise constitute a crime? Existing corporate liability doctrines, vicarious liability, the identification doctrine, and organisational fault models struggle to accommodate this new reality.

*PhD, FCIA. Associate Professor of Criminal Law University of Abuja. Email: gloria.shjaobi-ibikunle@uniabuja.edu.ng, Tel: +234 80 3422 5918.
**PhD, Company Secretary and Legal Adviser, Nigerian University Pension Management Company, Email: derebipi@gmail.com, Tel: +23480 06074124

[1] M E Diamantis, 'The Extended Corporate Mind: When Corporations Use AI to Break the Law' (2020) 98 *North Carolina Law Review* 893. https://scholarship.law.unc.edu/nclr/vol98/iss5/2. Accessed 26th August 2025.

[2]

2.0 Theoretical Framework

Corporate criminal liability is premised on the recognition that corporations, though artificial entities, can commit crimes through the acts of their agents. Three principal doctrines have emerged across jurisdictions viz:

2.1 Vicarious Liability (United States of America Model)

The US employs a broad vicarious liability *(respondeat superior)* doctrine for corporate crimes. A corporation can be criminally liable for any offense committed within the scope of employment and at least in part to benefit the company.[3] This approach imputes liability on a corporation for acts committed by employees within the scope of their employment. This expansive rule means U.S. prosecutors have historically had an easier time imputing liability to companies than their UK counterparts. However, AI-driven misconduct tests the limits of *respondeat* superior. Vicarious liability requires a human "agent" who committed the crime. If an AI system operating autonomously causes a violation without a specific employee's direction or intent, then *"under current law, corporate criminal liability cannot be based on the actions of an agent that is an artificial entity."*[4] In these instances, no human possesses the requisite mens rea, and current legal frameworks do not recognize an AI entity as capable of forming intent. Recent developments have proposed that actions taken by a corporation's AI systems be attributed to the corporation itself, such as interpreting algorithmic "knowledge" as corporate knowledge.[5] The U.S. framework, while more flexible than the UK's, faces a *mens rea* attribution gap in the age of AI – one that may require doctrinal evolution or creative charging (such as negligence-based offenses or strict liability regulatory crimes) to fill. The doctrine prioritises deterrence but has been criticised for being overly expansive, effectively punishing corporations even where senior management did not

[3] L Tsao, *et al*, 'Corporate Criminal Liability for Artificial Intelligence' *Law.com* (21 May 2024) https://www.law.com accessed 26 August 2025.
[4] *ibid*
[5] ME Diamantis, 'The Extended Corporate Mind: When Corporations Use AI to Break the Law' (2020) 97 *North Carolina Law Review* 893, available at SSRN https://ssrn.com/abstract=3422429 or http://dx.doi.org/10.2139/ssrn.3422429 accessed 26 August 2025.

know of the offence. It is unclear whether autonomous algorithmic decisions, absent human input, can be imputed to the corporation. Although this doctrine has allowed extensive prosecution of corporate misconduct, as in *United States v Bank of New England*[6]. However, with autonomous AI systems, the doctrine faces challenges viz, algorithms are not "employees", nor can they form intent in the human sense.

2.2 Identification Doctrine (United Kingdom Model)

Liability is attributed where the "directing mind and will" of the company, typically directors or senior executives, commits the offence. This was established in *Tesco Supermarkets Ltd v Nattrass,*[7] where the House of Lords held that liability attaches only when senior officers embodying the company's mind are implicated. In a recent case, however, the Serious Fraud Office failed to prosecute Barclays PLC for alleged fraud because it could not link the wrongdoing to a single high-level individual under the identification test.[8] AI systems exacerbate this challenge such that, if an algorithm makes a wrongful decision (e.g., an AI trading program manipulates markets or an underwriting AI unlawfully discriminates), there may be no individual director with the requisite mens rea. The UK government, recognizing these gaps, in 2023, introduced reforms via the Economic Crime and Corporate Transparency Act.[9] including a new "failure to prevent fraud" offense and plans to broaden the identification doctrine for certain economic crimes.[10] The "failure to prevent" model imposes liability on companies for crimes by associated persons (including potentially AI acting under company control) unless they can show adequate prevention measures. This shift bypasses the need to find a directing mind. There is also growing discussion of moving toward models that consider corporate culture or management failure[11] to hold companies accountable when organizational systems (potentially including AI governance systems) encourage wrongdoing. These

[6] 821 F.2d 844 (1st Cir. 1987).
[7] (1972) AC 153
[8] Shepherd and Wedderburn LLP, 'Corporate Manslaughter and Corporate Homicide Act 2007' *Lexology* (25 September 2007) https://www.lexology.com accessed 26 August 2025
[9] Economic Crime and Corporate Transparency Act 2023, s 2
[10] Economic Crime and Corporate Transparency Act 2023, c 56.
[11] UK's Corporate Manslaughter and Corporate Homicide Act 2007.

adaptations reflect an acknowledgment that strict identification doctrine is ill-suited for AI-era corporate criminality.[12]

The UK model, rooted in the identification doctrine, has faced sustained criticism in the context of complex corporate structures. Large corporations can diffuse decision-making such that no single individual qualifies as the "directing mind." Also, attributing *mens rea* to AI-generated decisions is problematic, as there is no human directing the mind, only a small set of top executives qualify as the "directing mind," which makes it too difficult to convict large corporations, particularly when decision-making is distributed or automated.[13] The Corporate Manslaughter and Corporate Homicide Act 2007 represents a shift toward organisational liability by focusing on systemic management failures, but it remains limited to health and safety contexts. This, in the AI context, attributing intent or recklessness remains unresolved.

2.3 Nigeria: Alter Ego Doctrine and Emerging Perspectives

Nigeria's corporate criminal liability doctrine largely follows the English common law tradition, emphasizing the alter ego (identification) theory for offenses requiring intent.[14] As Nigerian courts have stated, criminal intent of companies is established by attributing the *mens rea* of high-ranking officers to the company, mirroring the UK's "directing mind" approach.[15] This means Nigerian corporations historically could be convicted for crimes of intent only if a directing officer or "alter ego" was personally culpable. Nigeria also recognizes vicarious liability for strict liability and regulatory offences, but for serious crimes involving intent, the identification theory remains primary.[16] This poses similar challenges in AI scenarios such as, if an AI system deployed by a Nigerian

[12] Squire Patton Boggs, 'The Corporate Manslaughter and Corporate Homicide Act 2007' *Lexology* (21 December 2007) https://www.lexology.com accessed 26 August 2025

[13] Edmonds, Marshall and McMahon, 'Expanding Corporate Criminal Liability: What Does This Mean for Businesses?' *Lexology* (2 April 2025) https://www.lexology.com/library/detail.aspx?g=50f098e7-c896-4865-acfe-e2203ea3c912 accessed 19 August 2025.

[14] K.O Mrabure and A. Abhulimhen-Iyoha, 'Corporate Governance and Protection of Stakeholders Rights and Interests' (2020) 11 *Beijing Law Review* 292–308, DOI: 10.4236/blr.2020.111020

[15] *ibid*

[16] K.O Mrabure and A. Abhulimhen-Iyoha**, 'A** Comparative Analysis of Corporate Criminal Liability in Nigeria and Other Jurisdictions' (2020) 11 *Beijing Law Review* 429–443, DOI: 10.4236/blr.2020.112027

company engages in wrongdoing (for instance, an algorithmic decision platform violating consumer protection laws), it may be difficult under current law to pin responsibility on the company unless one can show a directing officer knew or intended that outcome. Mrabure and Abhulimhen-Iyoha [17] note that requiring a crime to be traced to a high-ranking manager is an impediment in combating modern corporate crime, since large companies can diffuse decision-making to avoid liability. In practice, while there are calls for clearer guidelines on corporate accountability for AI, regulators like the Nigerian SEC have shown proactive interest; urging the use of AI in surveillance to police illicit corporate activity such as crypto asset abuses. During the West Africa Compliance Summit in Cape Verde, Nigeria's Securities and Exchange Commission (SEC) Director-General Dr Emomotimi Agama emphasized the deployment of AI-powered blockchain analytics tools. These tools are intended to monitor illicit transactions, safeguard market integrity, and protect consumers, especially in the expansion of the digital asset space.[18] Additionally, the Punch reported that the SEC plans to deploy AI surveillance tools for blockchain analytics to trace illicit activity, further affirming the commission's forward-leaning approach to enforcement in crypto markets.[19] This was positioned as a necessary strategy for transitioning Nigeria's capital market oversight from a reactive approach to a predictive, technology-enabled model, directly aimed at combating fraud and systemic risks.[20] In summary, Nigeria's doctrine is still rooted in traditional alter ego and vicarious liability principles, but there is recognition that these must adapt to address the complexities introduced by AI-driven decisions.

3.0 AI as a Tool for Corporate Crime

Artificial intelligence is increasingly deployed as a powerful instrument in corporate operations. However, the same features that make AI attractive for efficiency and

[17] *ibid*

[18] Dr Emomotimi Agama (Director General, Nigerian SEC), speech at the West Africa Compliance Summit, Cape Verde (4 August 2025), on the use of AI-powered blockchain analytics for monitoring illicit transactions.

[19] 'SEC flags $2.1 bn suspicious crypto deals across W'Africa', The Punch (4 Aug 2025), reporting the SEC's plans to deploy AI surveillance tools for blockchain analytics

[20] Dr Emomotimi Agama (Director-General, Nigerian SEC), Fellowship Inaugural Lecture of the Capital Market Academics of Nigeria, via News Agency of Nigeria (1 Jul 2025), calling for the adoption of AI-driven surveillance systems for predictive regulation of the capital market.

profitability, viz; speed, autonomy, and predictive accuracy, also make it a potential enabler of corporate criminality.

3.1. Algorithmic Trading and Market Manipulation

AI is widely used in financial markets for high-frequency and algorithmic trading. While such technologies can improve liquidity and efficiency, they also create risks of market manipulation. For instance, AI-driven trading programs may engage in "spoofing" (placing and canceling trades to mislead markets) or contribute to flash crashes, where rapid automated trading destabilises markets. In such cases, proving corporate liability is complicated, since the harmful conduct may result from the machine's learning patterns rather than human instruction[21].

3.2 Price-Fixing and Algorithmic Collusion

Competition authorities have expressed concern about the capacity of AI to facilitate tacit collusion between corporations. Algorithms can monitor rivals' prices and automatically adjust to maximise profits, creating cartel-like outcomes without any explicit human agreement.

3.3 Money Laundering and Financial Crime

AI tools designed for transaction monitoring can paradoxically be repurposed to evade detection, enabling complex money laundering schemes. For example, corporations may use AI to identify regulatory blind spots, structure illicit transactions, or exploit weaknesses in anti-money laundering systems[22].

3.4 Cybercrime and Data Breaches

AI can also be misused to conduct cyberattacks, hack sensitive data, or exploit vulnerabilities in rival corporate systems. Such conduct, if perpetrated by or on behalf of a corporation, falls squarely within the scope of cybercrime and corporate liability.

[21] M E Diamantis, 'The Extended Corporate Mind: When Corporations Use AI to Break the Law' (2020) 98 *North Carolina Law Review* 893, 915–918

[22] F G Palazzo and A Deffains, 'Artificial Intelligence and the Risk of Money Laundering' (2021) 27 *Journal of Money Laundering Control* 34, 38–41

Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act[23] criminalises corporate involvement in such offences, but the statute does not directly address scenarios where AI autonomously executes attacks. Furthermore, there's no specific mention of AI attribution, autonomous systems liability, or machine-driven cyber offences.

4.0 AI as a Perpetrator

The more difficult question in corporate criminal law is whether artificial intelligence can itself be regarded as a perpetrator of crime. Unlike human agents, AI systems operate without consciousness, intent, or moral blameworthiness. Yet, their capacity for autonomous decision-making raises the possibility that they may directly "commit" acts that satisfy the actus reus (physical element) of an offence, even where no human actor intended the outcome[24].

4.1 The *Mens Rea* Dilemma

Traditional criminal liability requires proof of a guilty mind (mens rea). However, AI systems cannot form intent in the human sense. This challenges liability doctrines which rely on attributing criminal intent to a corporate officer. The identification doctrine, for instance, presumes a human directing mind[25].

4.2 AI and the Electronic Personhood

The idea of granting AI systems electronic personhood has been proposed. The European Parliament, in a 2017 resolution, controversially suggested that sophisticated autonomous systems could be granted a legal status similar to corporate personhood, enabling them to bear responsibility for harm caused.[26] While this could address gaps in accountability,

[23] Cybercrimes (Prohibition, Prevention, etc.) Act 2015; Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act 2024; s 6 (unauthorised access and hacking); s 21 (mandatory reporting of cyber-incidents within 72 hours).

[24] V Mongillo, 'Corporate Criminal Liability for AI-Related Crimes: Possible Legal Techniques and Obstacles' (2023) 94 *Revue Internationale de Droit Pénal* 97, 105–107

[25] J Gobert, 'Corporate Criminality: Four Models of Fault' (1994) 14 *Legal Studies* 393, 397–400

[26] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [2018] OJ C252/239, para 59(f).

critics argue it risks shielding corporations from liability by shifting blame onto electronic agents that lack assets or deterrent capacity.[27]

4.3 Corporate Liability for Autonomous Acts.

An alternative approach is to treat AI as an instrument of the corporation, even when its decisions are autonomous. Under this view, deploying AI constitutes a corporate choice, and the company should remain liable for the foreseeable risks associated with its use. This aligns with the precautionary principle in corporate governance, whereby organisations must anticipate and mitigate risks created by technology under their control[28].

In Nigeria, corporate criminal liability is primarily governed by the Companies and Allied Matters Act 2020 (CAMA), the Economic and Financial Crimes Commission (Establishment) Act 2004 (EFCC Act), and the Cybercrimes (Prohibition, Prevention, etc.) Act 2015. These statutes enable corporate prosecution for offences such as fraud, cybercrime, and money laundering. However, none expressly contemplates autonomous decision-making by AI systems. For instance, while the Cybercrimes Act criminalises corporate involvement in cyberattacks, it presumes direct or indirect human conduct. This creates a regulatory lacuna where harmful acts are generated by unsupervised algorithms.

5.0 Legal and Regulatory Challenges

The rise of artificial intelligence in corporate operations exposes significant gaps in existing legal frameworks on corporate criminal liability. While many jurisdictions recognise that corporations can be held criminally accountable, AI-driven misconduct raises novel questions of attribution and enforcement. A foremost difficulty is the problem of attributing legal fault. Most criminal and regulatory regimes assume a human actor with intent or negligence. When an AI system is involved, identifying who (if

[27] A. Bertolini, 'Robots as Products: The Case for a Realistic Analysis of Robotic Applications and Liability Rules' (2013) 5 *Law, Innovation and Technology* 214, 233–35.

[28] L De Koker and M J Radović, 'Artificial Intelligence and Financial Crime: Europe and Beyond' (2022) 30 *European Journal of Crime, Criminal Law and Criminal Justice* 143, 154–156.

anyone) possessed the *mens rea* can be elusive.[29] This creates an enforcement gap and serious harm might occur, yet no one can be readily held criminally liable. Regulators are thus forced to get creative, turning to alternative enforcement tools such as civil penalties, strict liability offenses, or "failure to prevent" style charges that focus on corporate controls rather than intent.

Another challenge is evidentiary and technical. AI systems are "black boxes", often complex and opaque even to their creators. Regulators face hurdles in investigating AI-related misconduct because they may lack the expertise or legal authority to audit algorithms. The opacity of AI makes it hard to pinpoint wrongdoing or to demonstrate that a certain outcome was not just a bug but a foreseeable risk the company failed to mitigate. Despite increasing recognition that regulators need new tools, overseeing AI remains challenging because these systems can evolve unpredictably, even for their operators[30]. Jurisdictional issues further complicate enforcement. AI systems and digital services transcend borders, meaning an AI-related offense can have multi-jurisdictional facets. This highlights a broader challenge as without coordinated international frameworks, AI-driven corporate misconduct can fall between the cracks of national legal systems.

Finally, enforcement priorities and resource constraints play a role. Regulators might hesitate to bring test-case prosecutions on novel AI issues due to uncertainty in law and the high costs of litigation with well-resourced corporate defendants. Instead, there is preference for settlements or regulatory guidance rather than seeking a verdict on algorithmic discrimination.[31]

---

[29] European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)) [2018] OJ C 252/239, para 59(f).

[30] OECD, Criminal Liability of Legal Persons for Artificial Intelligence Involvement in Corporate Offences (2023) 8–10

[31]'AI bias in housing algorithms prompts settlement', AP News (10 May 2023) https://apnews.com/article/1bc785c24a1b88bd425a8fa367ab2b23 accessed 21 August 2025;Casualty Actuarial Society, Regulatory Perspectives on Algorithmic Bias and Unfair Discrimination (August 2024) https://www.casact.org/sites/default/files/2024-08/Regulatory_Perspectives_on_Algorithmic_Bias_and_Unfair_Discrimination.pdf accessed 26 August 2025.

While International bodies have started to address the regulatory implications of AI,[32] these frameworks focus more on civil and administrative liability rather than criminal responsibility.

5.1 Recent AI-Driven Corporate Misconduct Cases

Despite being a relatively new phenomenon, the past ten years offer telling case studies of AI-related corporate misconduct and regulatory action across jurisdictions:

5.2 United States – Algorithmic Bias in Housing Ads (Meta/Facebook)

In June 2022, the U.S. Department of Justice filed a landmark case against Meta (Facebook) for algorithmic discrimination under the Fair Housing Act.[33] Facebook's advertising algorithms were found to be selectively targeting housing ads in ways that excluded users based on protected characteristics like race and sex – essentially a machine-learning tool that perpetuated housing discrimination. Meta settled the case by agreeing to overhaul its algorithms and eliminate certain AI ad tools[34] This case study underscores that AI can lead to corporate civil-rights violations, and regulators will intervene to hold companies accountable for biased outcomes caused by their AI systems. It also illustrates how U.S. authorities are crafting remedies (algorithmic audits, system changes) to address harm without criminally prosecuting the algorithm as such.

5.3 United Kingdom – Algorithmic Trading Glitch (Citigroup Fine)

In May 2024, the UK Financial Conduct Authority (FCA) fined Citigroup's London subsidiary £27.7 million for failures in its algorithmic trading controls. The case arose from a 2022 incident where a trader's mistake (a single extra digit) caused Citigroup's automated trading algorithm to execute a massive $1.4 billion unintended sell order,

[32]OECD, 'Recommendation of the Council on Artificial Intelligence' (22 May 2019) OECD/LEGAL/0449 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
accessed 12 August 2025; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 910/2014, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) [2024] OJ L168/1.

[33] 'What to Expect in 2025: AI, Legal Tech and Regulation – 65 Expert Predictions' National Law Review (2 January 2025) https://natlawreview.com/article/what-expect-2025-ai-legal-tech-and-regulation-65-expert-predictions accessed 15 August 2025.

[34] *ibid*

briefly distorting European stock markets.[35] The FCA found that Citigroup's systems lacked proper safeguards, and that the algorithm was not prevented from flooding the market due to deficient "fat-finger" controls and ineffective real-time monitoring.[36] While this was not a deliberate crime, it was a regulatory breach of UK market conduct rules. The enforcement is instructive: regulators treated the AI trading system as part of the corporate "conduct," penalizing the firm for failure to have adequate risk management for its AI[37]

5.4 Nigeria – Data Analytics and Election Manipulation (Cambridge Analytica)

One of Nigeria's most prominent tangles with AI-driven corporate misconduct emerged from the 2015 elections. Cambridge Analytica, a now-infamous UK-based data analytics firm, was hired to influence Nigeria's 2015 presidential campaign using illicit means. Reports revealed the firm was paid around £2 million by political interests to orchestrate a vicious online campaign against the opposition candidate, including exploiting hacked personal emails and micro-targeted disinformation.[38] The case highlights transnational corporate malfeasance involving AI and underscores the need for cooperation between jurisdictions to address corporations that deploy AI for illegality across borders.

6.0 Corporate Governance and Compliance

Corporate governance frameworks play a critical role in managing the risks associated with artificial intelligence in corporate operations. As corporations increasingly integrate AI into decision-making processes, the responsibility of boards and management to oversee ethical, lawful, and transparent use of technology becomes paramount[39].

---

[35] Financial Conduct Authority, Artificial Intelligence (AI) Update **(**22 April 2024) https://www.fca.org.uk/publications/corporate-documents/artificial-intelligence-ai-update-further-governments-response-ai-white-paper accessed 26 August 2025; Financial Conduct Authority, AI Live Testing: The use of AI in UK financial markets (1 August 2025) https://www.fca.org.uk/news/blogs/ai-live-testing-use-ai-uk-financial-markets-promise-practice accessed 26 August 2025.

[36] *ibid*

[37] Financial Conduct Authority, Artificial Intelligence (AI) update – further to the Government's response to the AI White Paper **(**22 April 2024**)** https://www.fca.org.uk/publications/corporate-documents/artificial-intelligence-ai-update-further-governments-response-ai-white-paper. accessed 21 August 2025.

[38] *ibid*

[39] T. C. Li, 'Corporate Governance and AI: Board Duties in the Age of Algorithms' (2021) 44 *Seattle University Law Review* 1023, 1030–1034

6.1 Role of Boards

Directors owe fiduciary duties of care and oversight to ensure that corporate activities comply with the law. The Nigerian Code of Corporate Governance 2018 (NCCG)[40] emphasises the responsibility of boards to implement effective risk management systems. Boards therefore have a duty to oversee how AI is deployed, ensuring that its use aligns with compliance and ethical standards.

6.2 Compliance Programs

Effective compliance programs are essential for mitigating the risks of AI-driven misconduct. These include regular audits of algorithms, clear accountability structures, whistleblowing channels, and employee training on responsible AI use. Such measures demonstrate corporate commitment to due diligence and may mitigate liability[41].

6.3 Internal Controls and Whistleblowing

Corporations must develop mechanisms to detect and prevent AI misuse. Whistleblowing frameworks can provide early warnings of improper conduct, while internal audits can uncover algorithmic biases or vulnerabilities. Internationally, the OECD has highlighted the importance of accountability and transparency in AI governance[42].

7.0 Conclusion

Artificial Intelligence offers unprecedented benefits to corporate operations but also poses serious challenges to legal accountability. The use of AI in corporate crime, whether to facilitate fraud, evade controls, or inadvertently cause harm, has exposed fault lines in our liability frameworks. The UK, U.S., and Nigeria each illustrate facets of this emerging problem: from the constraints of outdated doctrines like identification, to the blind spots of vicarious liability, to the need for developing economies to catch up with governance of AI. Regulators and lawmakers are awakening to these issues, as seen by

[40] Financial Reporting Council of Nigeria, Nigerian Code of Corporate Governance 2018, Principle 23.1.
[41] R. Brownsword and M. Goodwin, *Law and the Technologies of the Twenty-First Century* (CUP 2012) 189–192.
[42] G. Szego, 'Artificial Intelligence and Whistleblowing: Enhancing Accountability in Automated Decision-Making' (2021) 37 *Computer Law & Security Review* 105412

new offenses. The overarching trend is a push to adapt accountability mechanisms so that companies cannot escape liability simply because misconduct was driven by an algorithm.

Moving forward, the interplay between AI and corporate criminality will demand ongoing vigilance and adaptation. Laws will likely evolve to clarify that delegating decisions to AI does not dilute a company's responsibility; if anything, it heightens the duty of care in oversight. International cooperation will be key, given the borderless nature of AI services and corporate structures. And within companies, governance must evolve a "duty of algorithmic care," integrating legal compliance into the AI development pipeline. Ultimately, maintaining the rule of law in the age of AI will require what one commentator calls a hybrid of **"**new tools for new crimes" and recommitting to fundamental principles: that corporate power, whether exercised by humans or artificial agents, must be accountable to societal norms and regulations.[43] The coming years will be pivotal as academia, industry, and government work together to ensure that artificial intelligence becomes not a loophole for corporate impunity, but simply another facet of corporate conduct that the law can govern and guide. Thus, this article recommends the following mechanism:

8.1 Updating Legal Doctrines

This involves expanding the theories of corporate liability to explicitly encompass AI conduct. This could mean courts imputing mens rea to a corporation if an AI's programming reasonably implies a decision to break the law. Another concept floated is recognizing "systems intentionality" or corporate culture such that, if an AI crime occurs due to a company's culture of inadequately controlling technology, the company could be liable by virtue of those cultures.

[43] A Glaubitz, *Algorithmic Liability: A Tort Law Perspective* (Yale University, 2021) https://politicalscience.yale.edu/sites/default/files/glaubitz_alina.pdf accessed 17 August 2025.

8.2 Legislation and Guidelines

Government should actively craft laws to regulate AI. The European Union's AI Act (expected to take effect in 2025–26) will impose strict obligations on developers and users of high-risk AI systems, including requirements for transparency, risk assessment, and human oversight. While the AI Act is primarily a regulatory scheme (with fines for non-compliance), it indirectly bolsters accountability. Companies deploying AI in fields like finance, safety, or employment must prevent harm or face penalties. The EU is also working on an AI Liability Directive to ease the ability of victims to sue companies for AI-caused damage, which complements enforcement by creating private accountability mechanisms. A key innovation across many jurisdictions is transparency mandates. This requires companies to disclose how their AI systems make decisions (especially when those decisions affect consumers or markets) and to conduct audits for bias or risk. This would assist both regulators and external stakeholders in holding companies accountable.

8.3 Strengthening Regulatory Capacities

It is recommended to create dedicated "AI oversight units" within agencies (for example, an AI task force at the SEC or a tech laboratory at Nigeria's SEC) to develop expertise in auditing algorithms. Regulators may also adopt new investigative tools, such as requiring companies to maintain algorithmic decision logs or incident reports that must be submitted upon request. Improved international cooperation is also emphasized and the creation of bilateral or multilateral agreements for data sharing in investigations of AI-related fraud or cybercrime to address jurisdictional hurdles. It is also essential for members of the judiciary to receive training on artificial intelligence to effectively address issues and render judgements in AI-related cases.

8.4 Corporate Governance and Ethical AI

The solution is not only legal but also organizational. Corporate governance reforms could require boards of companies to oversee AI risks as part of their fiduciary duty. It has become expedient for the Law to apply a duty of care when directors approve AI-driven technology to ensure accountability. Regulators should also ensure that the Board members receive continuous and relevant training on AI and advocate for ethical AI

frameworks; internal policies that commit companies to principles like fairness, accountability, and transparency. Nigeria's financial regulators, through PenCom and the central bank, have promoted responsible AI use in fintech and pensions, highlighting that firms should proactively prevent AI-driven errors or biases in customer services.[44] Crucially, there is an understanding that law alone must be coupled with proactive corporate responsibility; Companies need to invest in compliance and ethics for AI just as they do for human employees. The hope is that through a combination of legal reform, regulatory innovation, and corporate culture change, the gaps in accountability for AI-driven misconduct will gradually close, ensuring that advanced AI technologies are used responsibly and that corporations remain answerable for the actions of their machines as well as their people.

[44] Dr Emomotimi Agama (Director General, Nigerian SEC), Fellowship Inaugural Lecture of the Capital Market Academics of Nigeria, via News Agency of Nigeria (1 July 2025), calling for adoption of AI-driven surveillance systems for predictive regulation of the capital market.