

ARTIFICIAL INTELLIGENCE AND CORPORATE CRIMINAL LIABILITY: A COMPARATIVE APPRAISAL*

Abstract

Artificial intelligence is transforming corporate activity and calling established doctrines of corporate criminal liability into question. This research responds to the doctrinal uncertainty which exists regarding attribution of mens rea and actus reus given the context where autonomous systems have been deployed by corporations. It seeks to arrive at a consistent framework for assigning liability among corporations, programmers, and AI systems. The objectives of the article are to analyze current models across selected jurisdictions, detect doctrinal voids and suggest a normative standard rooted in corporate governance and technological accountability. Using a doctrinal and comparative legal methodology, the article examines statutes, case law and policy instruments from both common law and civil law systems. It proposes a new “algorithmic agency attribution theory”, which redefines AI as a functional extension of corporate intent but retains human oversight responsibilities. It walks through its thesis, which maintains that existing liability doctrines are inadequate but can be adapted to meet the challenges of using AI through principled reinterpretation. It also seeks to interrogate the confines of strict liability and vicarious liability in a world where machines can operate autonomously, making real-time probabilistic decisions. The article, therefore, adds to emerging scholarship by providing a model that achieves the dual objectives of innovation and criminal justice imperatives across global contexts; while proposing statutory clarification, robust compliance architectures and transnational regulatory harmonization to address the problem of corporate liability in an age of artificial intelligence.

Keywords: Artificial Intelligence; Corporate Criminal Liability; Comparative Law; Algorithmic Accountability; Legal Theory.

1. Introduction

The rise of AI as a transformative force in modern economies has introduced fundamental changes to how corporations operate and consequently brought about challenging questions related to corporate criminal liability. Corporate liability developed as a means of addressing the growing power and influence of corporate entities during the industrial revolution, in which legal systems struggled to attach criminal intent to non-physical entities.¹ The hesitance of courts to make corporations subject to criminal liability was from the orthodox view that a corporation could neither hold *mens rea* nor commit *actus reus* apart from its human agents.² The slow recognition of such doctrines as the identification theory would prove to be a watershed moment, opening the door for courts to impute the state of mind of senior officers directly onto the body corporate.³ In recent times, AI systems assets that make independent decisions, and thus constitute their own agents upended this framework by enabling non-human actors to participate in corporate structures. This will require a reexamination of fundamental legal principles, especially to the extent that AI systems work unpredictably or beyond the immediate control of human operators. Thus, the intersection of AI and corporate criminal liability is a new frontier for legal scholarship, requiring both doctrinal precision and creative theoretical innovations.

* **Prof M N UMENWEKE**, Professor of Law at Nnamdi Azikiwe University, Awka, Anambra State. E-mail: mn.umenweke@unizik.edu.ng Tel:08037090048.

¹J H Baker, *An Introduction to English Legal History* (Oxford: Oxford University Press, 2019), 512.

²A Wells, “Corporate Criminal Liability: A Ten Year Review,” *Criminal Law Review* (2018): 849.

³L H Leigh, *The Criminal Liability of Corporations in English Law* (London: Weidenfeld and Nicolson, 1969), 34.

Corporate criminal liability is supported through the historical evolution of legal personality and recognition (or lack thereof) that corporations are separate legal persons distinct from their members.⁴ This doctrine, firmly established by the landmark case of *Salomon v. Salomon & Co Ltd*,⁵ provided the doctrinal basis for treating corporations as subjects of law with rights and obligations. Courts eventually created tools like vicarious liability and strict liability to better punish corporate misconduct, especially in regulatory contexts and public welfare.⁶ These doctrines were meant largely to capture human-directed corporate actions, where control and accountability could point to specific actors. But as companies develop systems that allow for use of AI in corporate governance structures, this model becomes complicated when decision-making authority is obfuscated and diffused across complex algorithmic systems. Machine learning black boxes also make the attribution of liability much more challenging since AI driven conclusions may not be interpretable. This progression highlights the necessity for an adaptable legal framework that balances technological advancement with the demands of justice.

The acceleration of artificial intelligence technologies, especially those related to machine learning and autonomous systems, has given rise to new dimensions of risk within organizations.⁷ Robots are increasingly being used for automated decision-making in finance, healthcare and transportation, where some errors or system malfunction could cause much damage.⁸ Such systems have a degree of autonomy and their ability to self-adapt could challenge traditional ideas about control and foreseeability. This raises important issues about how accessible and liable corporations should be for the actions of AI systems that are developed beyond their initial programming.⁹ Moreover, the global nature of AI deployment hampers regulatory responses, as regulations around liability and accountability differ immensely from one jurisdiction to another. Not having an overarching legal regime creates ambiguity for companies operating in multiple jurisdictions, which could weaken both compliance and enforcement.¹⁰ The convergence of AI and corporate criminal liability therefore calls for a comparative and interdisciplinary approach to the relevant legal analysis.

In reaction to these challenges, legal scholars have started looking into new theoretical constructs for AI-related corporate liability.¹¹ Traditional theories, including identification theory, have faced challenges in explaining decentralized processes of decision-making involved in AI systems.¹² In a similar vein, vicarious liability regimes may not be fit for purpose where there is no identifiable human agent whose actions could be attributed to the corporation.¹³ Recent scholarship has accordingly highlighted the need for a pivot in models, toward ones that integrate elements of risk management and corporate culture as well as technological accountability. These strategies attempt to reconcile deterrence and fairness objectives, while noting the distinct properties of AI systems. In that sense, they stress the need for proactive compliance mechanisms such as algorithmic auditing and ethical

⁴P L Davies and S Worthington, *Gower's Principles of Modern Company Law* (London: Sweet & Maxwell, 2016), 72.

⁵*Salomon v. Salomon & Co Ltd* [1897] AC 22 (HL).

⁶C M V Clarkson, "Kicking Corporate Bodies and Damning Their Souls," *Modern Law Review* 59, no. 4 (1996): 557.

⁷S Russell and P Norvig, *Artificial Intelligence: A Modern Approach* (Harlow: Pearson, 2021), 28.

⁸European Commission, "Artificial Intelligence for Europe," <https://ec.europa.eu/digital-strategy/en/artificial-intelligence> (accessed March 18, 2026).

⁹F Pasquale, *The Black Box Society* (Cambridge, MA: Harvard University Press, 2015), 21.

¹⁰*Ibid.*, p.21

¹¹GHalley, *When Robots Kill: Artificial Intelligence under Criminal Law* (Boston: Northeastern University Press, 2013), 87.

¹²A Ashworth, *Principles of Criminal Law* (Oxford: Oxford University Press, 2020), 134.

¹³J Gobert and M Punch, *Rethinking Corporate Crime* (London: Butterworths, 2003), 98.

governance structures.¹⁴ The creation of such frameworks is a necessary step until the time when legal doctrine can catch up with technological reality.

Through a comparative legal analysis, significant variance in approaches adopted by jurisdictions towards corporate criminal liability is revealed in the context of emerging technologies.¹⁵ Common law systems (such as the ones in the United Kingdom and the U.S.) are often characterized by judicial doctrines and prosecutorial discretion, while civil law jurisdictions generally favor statutory regulation and administrative enforcement.¹⁶ The European Union has recently taken a proactive stance by putting forward complex regulatory frameworks for AI, challenging accountability provisions and risk classification among other things.¹⁷ By contrast, many developing jurisdictions continue to struggle with the building blocks of corporate regulation, much less artificial intelligence with the comparatist focus on finding models to identify best practices which might propel together systems towards regulatory harmonization. It also highlights the need for place-sensitive solutions that are aligned with the socio-economic conditions of various jurisdiction.¹⁸ In the end, a comparative lens yields important lessons for what existing legal architectures do well but also where they have fallen short.

This article employs a doctrinal and comparative legal methodology to probe the difficulties that artificial intelligence presents for corporate criminal liability, and put forward a cohesive framework for reform. It is based on the analysis of primary legal sources as statutes, judicial decisions and international regulatory instruments and secondary sources as academic literature and policy reports. Using a comparative lens involves looking at different jurisdictions within the common law/civil law continuum to highlight convergences and divergences in legal practice. It is significant in entering the growing body of scholarship on AI and law by providing a novel theory that takes into account current socio-technical realities. It also offers policy, regulatory and corporate actors that need to successfully navigate the complexities associated with AI-driven decision-making actionable recommendations. All in all, the study aims to facilitate a framework where legal standards and technological advancements can work in tandem to shape a digital economy that safeguards shareholder interests.

2. Conceptual and Theoretical Framework

2.1 Artificial Intelligence

AI systems are computational processes constructed to execute tasks demanding human-like properties such as learning, reasoning, and decision-making; their paradigmatic coming-of-age has transformed the legal debate on responsibility and control.¹⁹ The modern conception of AI goes far beyond rule-based programming; it includes machine learning and deep learning systems that operate with differing degrees of independence and are not necessarily predictable.²⁰ Yet as this shift occurs from deterministic to probabilistic systems, the implications for legal attribution are profound particularly where AI systems are embedded within operational decision-making streams that are corporate action.²¹ Artificial intelligence systems already are in use today by corporations in high stakes environments including financial trading, healthcare diagnostics and autonomous transportation, raising issues of foreseeability and fault. The lack of insight into algorithmic processes commonly referred to as the “black box”

¹⁴Ibid., p.98

¹⁵V UEzeani, “Corporate Criminal Liability in Nigeria: An Appraisal,” *Nigerian Law Journal* 12, no. 2 (2019): 45.

¹⁶J. Coffee Jr., “Corporate Criminal Liability: An Introduction and Comparative Survey,” <https://scholarship.law.columbia.edu> (accessed March 18, 2026).

¹⁷European Parliament, “Artificial Intelligence Act,” <https://www.europarl.europa.eu> (accessed March 18, 2026).

¹⁸Ibid.

¹⁹S Russell and P Norvig, *Artificial Intelligence: A Modern Approach* (Harlow: Pearson, 2021), 47.

²⁰T Mitchell, *Machine Learning* (New York: McGraw-Hill, 1997), 2.

²¹F Pasquale, *The Black Box Society* (Cambridge, MA: Harvard University Press, 2015), 30.

problem can be an additional barrier for legal review and evidentiary evaluation in criminal cases.²² To this end, AI raises new questions for established legal concepts of control, intention and causation that have long served as the foundation for liability frameworks. Therefore, it is important to have a nuanced conceptualization of AI in order to create a coherent theory of corporate criminal liability for this new age of intelligent systems.

2.2 Corporate liability and algorithmic accountability

The legal principle of corporate criminal liability is a mechanism for holding companies responsible for the compensatory punishment based on the collective actions of their organization as determined by court cases and legislative lawmaking.²³ Fundamental doctrines such as identification theory, vicarious liability and strict liability have been developed to close the conceptual lacunae between artificial legal personality and human agency.²⁴ These doctrines, however, assume a level of human control and intent that isn't necessarily there in AI driven decision-making contexts.²⁵ Hence, algorithmic accountability has arisen as a complementary framework focused on transparency, explainability, and governance of AI usage in corporate contexts. Accountability encompasses not just an ex-post account of who is at fault, but also ex-ante duties with respect to risk assessments, audits and governance of algorithmic processes. In this regard, corporations are increasingly expected to internalise the risks accompanying AI systems and put safeguards in place that mitigate harm.²⁶ Corporate liability and algorithmic accountability converge here, then, to offer a crucial foundation for reconceptualising legal responsibility in automated contexts.

2.3 Algorithmic Agency Attribution Theory

The theoretical framework of this study rests on a new construct, which shall be called, throughout the course of this article, the “algorithmic agency attribution theory”. This theory aims to re-establish the grounds for how we understand artificial intelligence systems in relation to corporate criminal liability within a coherent doctrinal and normative system.²⁷ This theory diverges from traditional models, which treat AI systems as passive tools rather than functional extensions of corporate agency, and allows for a more flexible approach to the attribution of liability.²⁸ It builds on the work of contemporary sociotechnical systems theorists who describe how human actors, technological artifacts and institutional structures are interdependent and co-constituted in shaping outcomes.²⁹ The framework further encompasses concepts of risk distribution theory, arguing that liability should rest with the party better able to avoid, prevent and mitigate harm caused by AI operation. In so doing, it rejects the binary separation of human and machine agency, instead is calling for a continuum of responsibility that acknowledges the complexity of modern corporate settings.³⁰ It also builds on established principles of corporate governance, highlighting the importance of internal controls, compliance mechanisms, and ethical oversight in mitigating algorithmic risks. In the end, the agency attribution theory for algorithmic entities represents a strong theoretical groundwork to tackle some dilemmas that AI poses under corporate criminal law.

The algorithmic agency attribution theory rests on three mutually supportive pillars of functional attribution, heightened corporate duty, and distributed responsibility, each addressing a key lacuna of

²² Mitchell, (n.20), pp.2-3

²³ C Wells, *Corporations and Criminal Responsibility* (Oxford: Oxford University Press, 2001), 115.

²⁴ J Gobert and M Punch, *Rethinking Corporate Crime* (London: Butterworths, 2003), 56.

²⁵ B Mittelstadt et al., “The Ethics of Algorithms,” *Big Data & Society* 3, no. 2 (2016): 4.

²⁶ Ibid pp.4-6.

²⁷ G Hallevy, *When Robots Kill: Artificial Intelligence under Criminal Law* (Boston: Northeastern University Press, 2013), 102.

²⁸ L Floridiet al., “AI4People-An Ethical Framework for a Good AI Society,” *Minds and Machines* 28, no. 4 (2018): 695.

²⁹ B Latour, *Reassembling the Social* (Oxford: Oxford University Press, 2005), 72.

³⁰ Ibid., p.72

existing legal doctrines.³¹ Under functional attribution, the actions taken by AI systems should legally be attributable to the corporation that deploys those systems as integral parts of a corporate decision-making process. Enhanced corporate duty is a legal obligation that mandates corporations to exercise greater diligence in the design, deployment and monitoring of AI systems than what may be required under traditional compliance obligations.³² Distributed responsibility reflects that liability might be distributed across different actors developers, operators, corporations based on their roles and capacities. These proposals together seek to balance the need for accountability with the complexities and decentralization that come with technology. It also stresses the need for evidentiary standards that are suitable given unique qualities of AI systems, such as their opacity and adaptability.³³ Through its propositions, the theory provides both a principled and practical manner to frame liability.

The algorithmic agency attribution theory can best be applied in the present study as a lens as well as a normative framework for evaluating existing legal doctrines and reform proposals.³⁴ It allows for a necessary critique of how old principles like *mens rea* and *actus reus* can be creatively configured in the context of corporate behaviour propelled by AI.³⁵ The comparative aspect of the study enables to put theory in practice in different legal systems and reinforces its adaptability and operational applicability across regulatory environments anywhere on a global scale.³⁶ The framework also guides policy recommendations, especially those related to statutory reform, corporate governance and international harmonization. The theory emphasizes the importance of interdisciplinary solutions to legal problems by contextualizing AI within an even broader socio-technical and legal framework. It also highlights the need to update legal codes with the rise of technology, so laws can be enforced and regulated effectively. In conclusion, the engagement with this theoretical framework merits a higher analytical depth and practical relevance to the study.

3. Traditional Doctrines of Corporate Criminal Liability

The foundations of this principal, which is that the wrongdoing and ascribed mental states of certain cognescenti in a corporation have made up the “directing mind and will” for the corporate body itself.³⁷ The doctrine was articulated in English law through cases such as *Tesco Supermarkets Ltd v. Natrass*³⁸ where the House of Lords had observed that only those agents which were part of the corporate persona could be objects or subjects on which to impute liability to a company. Historically, the identification doctrine was critical to overcoming the conceptual problem of applying *mens rea* to an artificial legal person, one that had neither consciousness nor intent.³⁹ Yet the doctrine assumes a narrow understanding of corporate authority, attributing liability only to top management and ignoring lower-level employees or decentralized decision making. When it comes to modern companies with intricate hierarchies and tech-integrated processes, this becomes even more severe. With the rise of AI systems, the doctrine becomes even more inscrutable as decision-making may no longer be attributed to identifiable human actors in senior positions.⁴⁰ Thus, the identification doctrine finds it difficult to

³¹RBrownsword, *Rights, Regulation, and the Technological Revolution* (Oxford: Oxford University Press, 2008), 89.

³²UPagallo, *The Laws of Robots* (Dordrecht: Springer, 2013), 65.

³³KYeung and M. Lodge, *Algorithmic Regulation* (Oxford: Oxford University Press, 2019), 121.

³⁴M Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford: Oxford University Press, 2020), 144.

³⁵A Ashworth, *Principles of Criminal Law* (Oxford: Oxford University Press, 2020), 156.

³⁶European Commission, “Ethics Guidelines for Trustworthy AI,” <https://digital-strategy.ec.europa.eu>. (accessed March 18, 2026).

³⁷L H Leigh, *The Criminal Liability of Corporations in English Law* (London: Weidenfeld and Nicolson, 1969), 45.

³⁸*Tesco Supermarkets Ltd v. Natrass* [1972] AC 153 (HL).

³⁹C Wells, *Corporations and Criminal Responsibility* (Oxford: Oxford University Press, 2001), 38.

⁴⁰*Ibid*, pp 38-39

address the realities of corporate life where authority is not so much concentrated as diffused and mediated through smart systems.

The identification doctrine is closely tied to the idea of vicarious liability, where companies can be held liable for their employees' torts committed in the course and scope of employment, even when senior management was not directly involved.⁴¹ This doctrine has been especially applicable in jurisdictions like United States, where courts have taken an expansive view on corporate liability under the doctrine of respondent superior.⁴² Vicarious liability generalizes the idea of corporate responsibility, recognizing that corporations act through a large corral of agents - not just the ones at the top of an organizational chart. However, the doctrine assumes a direct relationship between the employee's conduct and the business of the corporation, as well as a level of human agency that has faults and intent that can be assessed. From an AI perspective, these assumptions fall apart quickly because systems of this nature do not fit the legal definition of an employee or agent. Additionally, since AI-assisted conduct may not be easily tied to any one individual within the corporation, this undermines the doctrinal foundation for vicarious liability.⁴³ Thus, if vicarious liability does offer a broader framework than the identification doctrine, it is still at a loss when faced with the complexities introduced by autonomous technologies. Besides the corporate attribution doctrine, another major doctrinal development is strict liability: individuals cannot be attributed criminal responsibility based on *mens rea* but rather corporations can incur it notwithstanding the need to prove *mens rea* especially in regulatory offences aimed at protecting public welfare.⁴⁴ An example of the strict liability applied to environmental laws is that of some air pollutants, which can be used as a metric for any given sector or area.⁴⁵ This doctrine is based on a practical realization that demanding proof of intent in cases involving corporations can impede their efficient enforcement and deterrence. However, the use of strict liability in AI is problematic from a normative standpoint -especially with regards to fairness and proportionality issues. Due to the autonomous and adaptive aspects of AI systems, some consequences may not have been intended or even reasonably foreseeable at all by the enterprise.⁴⁶ Enforcing liability under such scenarios threatens to punish corporations for harms that result from complex technological processes beyond their direct control. Thus, while strict liability provides a helpful instrument for regulatory enforcement, its unchecked expansion to conduct driven by AI may lead to inequitable results and greatly impact the perceived legitimacy of the legal system.

When placed alongside the realities of today's decentralized, automated, and algorithm-driven corporate practices that often run counter to these traditional doctrines, their stark limitations come into sharper focus.⁴⁷ As more and more corporations depend on AI systems working without human intervention, the link between human agency and corporate conduct is increasingly fractured.⁴⁸ The identification doctrine does not encapsulate this reality because it is limited to the senior management; whereas vicarious liability suffers with the lack of a human agent whose acts can be put on the corporation. Technological causation, and the distribution of responsibility among the different actors involved in developing and deploying AI systems are at least broad in scope but all fall short of recognizing the particulars emerging here and there. These doctrinal shortcomings also reveal a basic disconnect between existing legal frameworks and the dynamic nature of corporate activity. They additionally highlight the necessity for an agile and contextually adaptive approach to liability that can

⁴¹J Coffee Jr., "Corporate Criminal Liability: An Introduction and Comparative Survey," <https://scholarship.law.columbia.edu> (accessed March 18, 2026).

⁴²N Buell, "The Blaming Function of Entity Criminal Liability," *Indiana Law Journal* 81, no. 2 (2006): 480.

⁴³J Gobert and M Punch, *Rethinking Corporate Crime* (London: Butterworths, 2003), pp. 71-73.

⁴⁴A Ashworth, *Principles of Criminal Law* (Oxford: Oxford University Press, 2020), 168.

⁴⁵*R v Prince* (1875) LR 2 CCR 154.

⁴⁶C Clarkson, "Strict Liability and the Criminal Law," *Law Quarterly Review* 105 (1989): 234.

⁴⁷K Yeung and M Lodge, *Algorithmic Regulation* (Oxford: Oxford University Press, 2019), 98.

⁴⁸F Pasquale, *The Black Box Society* (Cambridge, MA: Harvard University Press, 2015), 52.

cater to the intricacies of AI-based surroundings.⁴⁹ Lacking this kind of response, the law will increasingly drift from realities that it and its participants need to regulate.

Considering these challenges, it is necessary to reevaluate the sufficiency of existing doctrines on corporate criminal liability and search possible alternative regimes that accommodate or respond to the consequences deriving from AI integration.⁵⁰ This paper uses a doctrinal and comparative legal research approach. Through an investigation of statutory language, judicial pronouncements, and scholarly commentary, this research aims to discern trends of convergence and divergence in the treatment of corporate criminal liability in technologically advanced contexts. In addition, the methodological scope includes interdisciplinary insights, and leverages relevant concepts from computer-based studies, ethics, and socio-technical theory to inform legal discourse. This process allows for a deeper insight into the issues created by AI, while promoting recommendations that are informed and relevant to the context in which they occur. This analysis is important because it may help to shape and develop legal doctrine in a way that is innovative but also respects accountability.⁵¹ The research will also serve as a roadmap for future reforms to ensure that corporate criminal law remains meaningful and effective in our digital age.

4. Artificial Intelligence and the Problem of Attribution

The incorporation of artificial intelligence in corporate operation fundamentally undoes the tenets *actus reus* and *mens rea*, traditional foundations that have provided not only the basis for punishable crimes but civil liability as well.⁵² As the physical element of a crime, *actus reus* presupposes a clear and traceable human action, whilst *mens rea* needs proof of a culpable mental state that can be traced back to another legal subject.⁵³ Traditional corporate law is based on doctrines that relate human behavior and intent to the corporate cell. But this framework is complicated by the fact that AI systems often produce autonomous decision-making processes that are not directly controlled or even fully understood by human actors. The ability of AI systems to function autonomously undermines the assumption that every action taken by a corporation is attributable to a human decision maker.⁵⁴ This poses considerable evidentiary and doctrinal challenges in proving both the *actus reus*, or physical element, and *mens rea*, or mental element, of an offence. As a result, the architecture of criminal liability becomes increasingly strained against technologically mediated corporate conduct.

The most serious challenge presented by Artificial Intelligence systems is their autonomy, enabling them to make decisions without real-time human intervention thus complicating the attribution of responsibility.⁵⁵ Autonomous AI systems, particularly those based on machine learning, can adjust their behaviour according to data inputs and environmental changes, yielding outputs that were not explicitly written into them by their developers.⁵⁶ This degree of autonomy poses questions about whether such systems can be said to “act” for legal purposes and, if they do act, whose act that constitutes.⁵⁷ The lack of direct human control challenges the applicability of classic doctrines grounded in identifiable agents to impose liability. Furthermore, the delegation of decision-making authority to AI systems presents challenges in terms of accountability especially in contexts where corporate actors depend on perceived

⁴⁹GHallevey, *When Robots Kill: Artificial Intelligence under Criminal Law* (Boston: Northeastern University Press, 2013), 119.

⁵⁰M Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford: Oxford University Press, 2020), 201.

⁵¹European Commission, “Ethics Guidelines for Trustworthy AI,” <https://digital-strategy.ec.europa.eu> (accessed March 18, 2026).

⁵²A Ashworth, *Principles of Criminal Law* (Oxford: Oxford University Press, 2020), 92.

⁵³J Herring, *Criminal Law: Text, Cases, and Materials* (Oxford: Oxford University Press, 2021), 105.

⁵⁴C Wells, *Corporations and Criminal Responsibility* (Oxford: Oxford University Press, 2001), 63.

⁵⁵GHallevey, *When Robots Kill: Artificial Intelligence under Criminal Law* (Boston: Northeastern University Press, 2013), 131.

⁵⁶S Russell and P Norvig, *Artificial Intelligence: A Modern Approach* (Harlow: Pearson, 2021), 56.

⁵⁷UPagallo, *The Laws of Robots* (Dordrecht: Springer, 2013), 89.

objectivity or efficiency of algorithmic processes.⁵⁸ This convergence has been referred to as the “autonomy gap,” in which accountability becomes diluted through multiple layers of human and technological mediation. This creates an elemental difficulty in linking *actus reus* and *mens rea* to corporations due to the sustaining nature of autonomy.

Beyond autonomy, unpredictability adds another layer of difficulty to the attribution of criminal liability because it permeates with uncertainty and indeterminacy into corporate conduct.⁵⁹ Machine learning algorithms the most well-known types being the ones based on neural networks can produce results that are not entirely predictable even to those who invented them.⁶⁰ This unpredictability complicates the legal requirement of foreseeability generally, which is often a key factor in proving negligence or recklessness under criminal law. Where AI-derived processes are responsible for harmful outcomes, it is unlikely that the corporation could have reasonably foreseen and averted the harm.⁶¹ The necessity of matching probabilistic conclusions in AI implication also presents a causality problem, where outputs would also be based on interactions between the data products and algorithmic frameworks as you systematize within the environment.⁶² Additionally, the nature of AI systems to learn and adapt makes them difficult to predict, as they could behave in ways not accounted for or controlled by monitoring methods. These traits make traditional, fault-based models of liability increasingly ill-equipped to deal with harms caused by AI.

Another top concern is the black box nature of AI systems the opaque reasoning processes driving a given algorithm’s choices that can make legal scrutiny difficult.⁶³ Most sophisticated AI models, especially deep learning systems, are not easily human-interpretable so an explanation of how particular decisions were made is hard to come by.⁶⁴ Such opacity creates considerable difficulties in criminal proceedings, where burden of proof requires clear and convincing accounts for causation and intent.⁶⁵ The opacity of AI systems also impairs corporations’ ability to monitor and control their operations, thus eroding internal accountability mechanisms. From a legal standpoint, it raises questions of fairness and appropriateness in terms of being responsible for something and where there is no evidence to support wrongful actions. In addition, opacity can impede regulatory scrutiny in as much as regulators may not have the technical knowledge or access to assess complex algorithmic systems. This black box quality of AI thus poses a significant challenge to the application of traditional doctrines of corporate criminal liability.

These challenges together emphasize the limitations of current legal approaches to addressing what is attributable criminal behavior in AI-empowered corporations and call for a re-evaluation of foundational principles. The doctrinal focus on human agency as the basis of liability is becoming increasingly untenable in environments where decision-making has been distributed throughout complex socio-technical systems.

5. Comparative Jurisdictional Analysis

In Nigeria, corporations can be held criminally responsible, but the system is still developing and faces many challenges. Traditionally, corporate liability in Nigeria works by attributing the actions and intentions of individuals usually employees or directors to the company itself. In other words, a company is only criminally liable if a human agent acting on its behalf commits an offence.⁶⁶ This

⁵⁸Ibid. pp. 89-90

⁵⁹F Pasquale, *The Black Box Society*, 67.

⁶⁰Mitchell, *Machine Learning*, 14.

⁶¹A Ashworth, *Principles of Criminal Law* (Oxford: Oxford University Press, 2020), 148.

⁶²Ibid, p. 149

⁶³B Mittelstadt *et al.*, “The Ethics of Algorithms,” *Big Data & Society* 3, no. 2 (2016): 6.

⁶⁴KYeung and M. Lodge, *Algorithmic Regulation* (Oxford: Oxford University Press, 2019), 142.

⁶⁵M Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford: Oxford University Press, 2020), 178.

⁶⁶ Gloria Shajobi-Ibikunle and Deborah Oluwadamilola Shajobi Oseghale (n 1).

approach is similar to the UK's identification doctrine, which focuses on finding a person within the organisation who represents its "directing mind and will."⁶⁷ Nigerian courts have sometimes applied this principle strictly, but there are areas, particularly in regulatory offences, where liability can be imposed even without proof of intention, reflecting some flexibility in the law.²

Despite these foundations, Nigeria does not yet have a legal framework specifically designed for artificial intelligence or for holding corporations accountable for AI driven harms. Existing laws that touch on technology include the Cyber Crime Prohibition Act 2015, National Information Technology Development Agency (NITDA) Act 2007, the Nigeria Data Protection Act 2023, and sector-specific regulations in banking, telecommunications, and finance.⁶⁸ These rules are mainly concerned with data protection, privacy, and ethical use of technology rather than criminal liability for harm caused by AI. Scholars have pointed out that while these laws provide some guidance, they leave a large gap when it comes to emerging AI technologies, especially those that make autonomous decisions without direct human oversight.⁶⁹

At the same time, AI adoption in Nigeria is growing rapidly. Fintech companies, digital banks, telecom operators, and security firms are increasingly using AI for automated decision-making, surveillance, fraud detection, and customer service. While these technologies improve efficiency, they also create risks. Examples include algorithmic fraud, biased or discriminatory decisions, and automated financial misconduct. Because enforcement is weak and laws are not tailored to AI, there is a real possibility that companies could avoid accountability even when AI systems cause harm.⁷⁰

Several challenges make this problem even more difficult. First, Nigerian courts still rely heavily on human-centered doctrines similar to the UK's identification model, making it hard to hold corporations liable when no specific person can be blamed. Second, there is no comprehensive AI law to clarify responsibility for automated systems or set clear obligations for corporate governance. Third, regulatory and judicial institutions often lack the expertise and resources to enforce technology-related laws effectively. Finally, technology is evolving faster than the law, so corporations can deploy AI systems without clear legal guidance, increasing the risk of harm and accountability gaps.⁷¹

Overall, while Nigeria recognises corporate criminal liability in principle, the country faces significant legal and regulatory challenges when it comes to AI. The corporate criminal liability regime as applied to AI specifics presents both unique similarities and striking contrasts across common law, civil law, and nascent African jurisdictions; all of which reflect varying approaches to corporate criminality based in doctrinal preference/configurative priorities.⁷² In common law jurisdictions, the UK and USA, for instance, courts have historically relied on judicially developed doctrines such as those of identification and vicarious liability to determine corporate responsibility.⁷³ These systems preserve judicial flexibility for the courts, allowing them to develop existing doctrines piecemeal when needed by novel

⁶⁷Ibid.

⁶⁸Ayodeji Emmanuel Aimasiko, *The Constitutionality of Fine Imposition Under the Nigeria Data Protection Act, 2023 and its Implications* (International Journal for Public Policy, Law and Development, 2025) <https://ijpld.com/ijpld/article/view/29> accessed 22 March 2026.

⁶⁹Bamikole AP Folorunso, 'The Legal Status of Autonomous Cyber Agents: Rethinking Criminal Liability in the Age of AI' (2025) 2(1) *OMANARP International Journal of Law* 1 <https://acadrespub.com/index.php/oijl/article/view/153> accessed 21 March 2026.

⁷⁰Moses Peace Richard, 'Legal Perspective on the Use of Artificial Intelligence in Corporate Governance in Nigeria: Potentials and Challenges' (2024) 34(48) *Journal of Legal Studies* 97 <https://doi.org/10.2478/jles-2024-0016> accessed 21 March 2026.

⁷¹TI Kagbala, *Towards a Legal Framework for Regulating Artificial Intelligence (AI) in Nigeria* (2025) *International Journal of Advanced Legal Studies and Governance* <https://icidr.org.ng/index.php/Ijalsg/article/view/1816> accessed 22 March 2026.

⁷²J Coffee Jr., "Corporate Criminal Liability: An Introduction and Comparative Survey," <https://scholarship.law.columbia.edu> (accessed March 18, 2026).

⁷³C Wells, *Corporations and Criminal Responsibility* (Oxford: Oxford University Press, 2001), 77.

challenges related to AI-driven conduct.⁷⁴ Yet this kind of flexibility creates uncertainty wherein courts are required to bend established tenants and scopes of existing doctrines to the needs of non-humans decision-making systems. In contrast, civil law jurisdictions depend more on codified statutes and regulatory frameworks to shape corporate behavior and the risks of technology. African jurisdictions each have adopted common law traditions yet exist in varied socio-economic and institutional settings, resulting in a diversity of regulatory realities. For example, while Nigeria's Companies and Allied Matters Act⁷⁵ provides for the statutory basis of corporate liability, it still does not specifically mention AI-driven conduct in its provisions thus exposing a regulatory gap on emerging technology. This diversity underscores the importance of comparing these approaches to identify common challenges and possible context-specific solutions regarding AI-related corporate liability.

In the United States, corporate criminal liability is interpreted broadly through the doctrine of respondeat superior which permits corporations to be held liable for acts performed by employees while in the scope of their employment and for the benefit of the corporation.⁷⁶ This broad strategy aids law enforcement by easing the threshold for attribution and allowing prosecutors to confront a spectrum of kindred corporate failures, including those that are technologically intermediated.⁷⁷ However, the application of this doctrine to AI systems reveals conceptual weaknesses as AI entities do not conform comfortably within conventional categories of employees or agents.⁷⁸ Recent policy developments in the United States have thus focused on corporate compliance, algorithmic auditing and risk management as mechanisms for addressing AI-related harms. The emphasis is now on preventive governance rather than retrospective liability alone. However, the lack of a widely applicable federal legal framework dealing with AI and corporate criminal liability remains a source of regulatory fragmentation. As a consequence, the U.S. model is broad and flexible, but ultimately fails to tailor regulatory pathways efficiently to the complexities of autonomous systems.

The United Kingdom has taken a more restrictive approach by way of the identification doctrine, which has been subject to significant criticism and debate as it arguably fails to adequately encompass wrongdoing in large and technologically sophisticated corporate structures.⁷⁹ But efforts to shift the blame from individuals to organizations, like the Corporate Manslaughter and Corporate Homicide Act 2007, are also meant to expand what is considered corporate accountability.⁸⁰ But these reforms do not specifically address the specific challenges posed by artificial intelligence, and then specifically with regard to autonomy and algorithmic opacity. The UK Law Commission has acknowledged these limitations and recommended reform to modernize corporate criminal liability, including the creation of wider failure-to-prevent offenses.⁸¹ The legal framework has yet to fully adapt to the challenges posed by these new technologies, which rely on decentralized and AI-driven decision-making processes. This captures a wider tension in common law systems between doctrinal continuity and an impulse to generate new doctrines. As a result, the UK approach shows both the flexibility and shortcomings of traditional legal doctrines in addressing new technologies.

In contrast, within the European Member States, civil law jurisdictions have taken a more comprehensive and regulatory approach through recent initiatives such as the proposed Artificial

⁷⁴J Gobert and M. Punch, *Rethinking Corporate Crime* (London: Butterworths, 2003), 134.

⁷⁵Companies and Allied Matters Act 2020 (Nigeria), ss. 42, 65, 87, 305–311, 336, 548, <https://www.cac.gov.ng> (accessed March 19, 2026).

⁷⁶N Buell, "The Blaming Function of Entity Criminal Liability," *Indiana Law Journal* 81, no. 2 (2006): 473.

⁷⁷Coffee Jr., "Corporate Criminal Liability: An Introduction and Comparative Survey," <https://scholarship.law.columbia.edu> (accessed March 18, 2026).

⁷⁸G Hallevey, *When Robots Kill: Artificial Intelligence under Criminal Law*, 156

⁷⁹A Wells, "Corporate Criminal Liability: A Ten Year Review," *Criminal Law Review* (2018): 860.

⁸⁰ Corporate Manslaughter and Corporate Homicide Act 2007 (UK), s. 1, <https://www.legislation.gov.uk/ukpga/2007/19/section/1> (accessed March 19, 2026).

⁸¹ UK Law Commission, "Corporate Criminal Liability: An Options Paper," <https://www.lawcom.gov.uk> (accessed March 18, 2026).

Intelligence Act which aims to create a uniform AI governance framework across all member states.⁸² This framework is built around risk classification, transparency, and accountability, thus addressing many of the challenges posed by AI-fueled corporate behaviour.⁸³ The EU model stems from a preventive regulatory philosophy and into which rests the idea of mitigating risks before injury happens instead of relying only on criminal sanctions⁸⁴. In contrast, statutory developments such as the Companies and Allied Matters Act and section-specific regulations⁸⁵ have informed a common law framework in Nigeria, for example as a jurisdiction in Africa. Nigerian corporate criminal liability, however, does exist through doctrines of vicarious liability and statutory offense but lacks a comprehensive legal framework that deals with AI harms. So even as Nigeria embraces AI technologies, and pulls into the 21st century vis-a-vis banking services and telecommunications, if we do not place urgent regulations it is a disaster waiting to happen. In addition, constant shuffling with technical capacity and insufficient enforcement mechanisms exacerbate the challenge of effective governance of AI. The comparison of the two systems also highlights a broader trend, wherein advanced markets are increasingly developing regulations for hybrid initiatives and emerging countries seem to be unable to keep pace even with the compliance frameworks within business regulation.

A comparative synthesis of these jurisdictions demonstrates both similarities and differences in approaches to AI-related corporate criminal liability, pointing toward a developing international consensus regarding the need for doctrinal and regulatory reform.⁸⁶ The common law places great weight on flexibility and judicial innovation, while civil law jurisdictions emphasize codification and the discipline of preventive regulation, and both inherited doctrinal approaches as well as local realities have influenced African systems in hybrid form.⁸⁷ In response to the challenges posed by AI, across these systems we have started to see a trend towards integrating compliance-based models, risk governance frameworks and enhanced corporate oversight mechanisms.⁸⁸ While work in the field is making great strides, some critical gaps remain such as in the areas of attribution and ensuring transparency at every step of applying machine learning techniques to a real-world setting, where accountability may be less clear given the autonomous use of these algorithms within wider networks. The comparative analysis shows that while no jurisdiction has fully solved these issues, each offers important lessons of potential paths to reform. It also emphasises the significance of understanding legal solutions vis-à-vis particular institutional and developmental pathways. In the end, this part shows that a plausible model of corporate liability for AI should be simultaneously informed by global developments and adaptable to local conditions, straddling both doctrinal coherence and regulatory innovation.

6. Reforming Corporate Criminal Liability in the Age of AI

(i) Statutory Recognition of Algorithmic Agency

Legislators must create clearer legislative frameworks recognizing AI systems as an extension of corporate conduct: this is already being done by institutions like the National Assembly of Nigeria and the UK Parliament, which have enacted provisions making algorithms responsible under corporate attribution.

⁸²K Yeung and M Lodge, *Algorithmic Regulation* (Oxford: Oxford University Press, 2019), 165.

⁸³European Parliament, "Artificial Intelligence Act," <https://www.europarl.europa.eu> (accessed March 18, 2026).

⁸⁴V U Ezeani, "Corporate Criminal Liability in Nigeria: An Appraisal," *Nigerian Law Journal* 12, no. 2 (2019): 49.

⁸⁵Companies and Allied Matters Act 2020 (Nigeria), ss. 42, 65, 87, 305–311, 336, 548, <https://www.cac.gov.ng> (accessed March 19, 2026).

⁸⁶RBrownsword, *Rights, Regulation, and the Technological Revolution* (Oxford: Oxford University Press, 2008), 131.

⁸⁷M Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford: Oxford University Press, 2020), 209.

⁸⁸European Commission, "Ethics Guidelines for Trustworthy AI," <https://digital-strategy.ec.europa.eu> (accessed March 18, 2026).

Regulators, such as the Corporate Affairs Commission and UK Companies House can then implement these provisions through requirements for corporate registration and disclosure.

(ii) Mandatory Algorithmic Governance Frameworks

Companies ought to be mandated to build and run in-house AI governance systems under the supervision of regulators such as the Securities and Exchange Commission Nigeria, United States Securities and Exchange Commission, holding actors accountable for algorithmic decisions. Such frameworks should be equipped with mandatory audit and compliance reporting requirements, overseen by these agencies.

(iii) An Affordable Duty of Care as it Relates to AI Deployment:

Courts and regulatory authorities, including the Federal High Court of Nigeria and the UK Financial Conduct Authority should impose an enhanced duty of care on corporations to ensure that AI systems are thoroughly tested and monitored prior to deployment and during use. Civil and criminal liability should be incurred for this breach of the duty, strengthening preventive responsibility.

(iv) Liability Regime that is distributed among AI Ecosystem Actors

Advancing a distributed liability model for AI, enforced by the National Information Technology Development Agency (NITDA) and the European Commission, which can apportion accountability across developers, operators and corporate users of systems. This way liability corresponds with actual control and contribution to the harm through-out AI value chain.

(v) Mechanisms for regulatory oversight and certification

Generative AI systems that are high-risk should be submitted to independent oversight bodies (ideally one system for all generative AIs not limited by jurisdiction) who can designate and enforce certification regimes, akin to the National Information Technology Development Agency or the European Artificial Intelligence Board. These bodies should be empowered to impose sanctions, revoke certifications and limit operations when compliance standards are not met, thus reinforcing preventive regulation.

7. Conclusion and Recommendations

This article has critically explored the intersection of artificial intelligence and corporate criminal liability, proving that traditional doctrines such as identification, vicarious liability, and strict liability are becoming more insufficient at dealing with AI-induced corporate behavior. It explained that the most important problem is how autonomy, opacity and unpredictability makes it challenging to assign *actus reus* and *mens rea*. Through a comparative appraisal of common and civil law jurisdictions, alongside African worlds like Nigeria, the work outlined both accountabilities left between the seams of doctrine and incipient regulatory responses. The aim of the article was to put forth a novel algorithmic agency attribution theory as a more coherent framework for reconciling legal responsibility with the contemporary socio-technical realities. Finally, it finds that while we rely on our existing legal doctrines, these must be reinterpreted and supplemented in order to ensure that corporate accountability does not get undercut by technological innovation.

In the light of the above submission, the article proposes that:

Firstly, the legal systems need clear statutory provisions that explicitly make the corporation liable for AI driven actions in such a way that there is no ambiguity.

Secondly, regulatory authorities should require the establishment of strong algorithmic governance frameworks - encompassing auditing, transparency, and risk management mechanisms in corporate structures.

Thirdly, there must be an increased duty of care on corporations that use AI to prevent foreseeable risks from materializing through testing and monitoring.

Fourthly, liability regimes should adopt a distributed approach in which responsibility is assigned among all relevant actors involved in the AI ecosystem, including developers and operators.

Fifthly, the potential for establishing stronger evidentiary standards and inter-disciplinary research to create general guidelines that combine law, technology and ethics in order to help tackle corporate criminal liability in the age of AI.