MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 3796-3801

FROM BOARDROOMS TO BLACK BOXES: EXAMINING CORPORATE CRIME LIABILITY, AI-INDUCED MISCONDUCT, AND THE URGENT NEED FOR ADAPTIVE MANAGEMENT POLICIES AND REGULATORY OVERSIGHT

Dr. Kasturi Bhagat, LLD Scholar, India International University of Legal Education and Research (IIULER)
Tejaswini Dewangan, PhD Scholar, India International University of Legal Education and Research (IIULER)
Shreya Srivastava, PhD Scholar, India International University of Legal Education and Research (IIULER)

ABSTRACT
The rapid integration of artificial intelligence into corporate decision-making processes has fundamentally transformed the landscape of corporate governance and liability. Traditional doctrines of corporate criminal liability, rooted in human intent, agency principles, and hierarchical control, are increasingly strained when confronted with autonomous, opaque, and self-learning systems. This research critically examines how AI-induced misconduct challenges existing legal frameworks governing corporate crime, particularly in relation to attribution of mens rea, foreseeability, and organizational faults. It explores the doctrinal evolution of corporate liability from identification theory to aggregation and corporate culture models and evaluates their adequacy in addressing harms caused by algorithmic decision-making systems. Further, the paper analyses emerging instances of AI-related corporate misconduct, including algorithmic collusion, discriminatory automated decision-making, and compliance failures in fintech and data-driven enterprises. By drawing on comparative perspectives from jurisdictions such as the United States, the European Union, and India, the study identifies regulatory gaps and inconsistencies in addressing AI-driven risks. It argues that existing compliance mechanisms, largely designed for human-controlled misconduct, are insufficient to govern autonomous systems that operate beyond direct managerial oversight.
Keywords: Corporate Criminal Liability, Artificial Intelligence, Algorithmic Accountability, Corporate Governance, Compliance, Mens Rea, Autonomous Systems, Regulatory Oversight, AI Ethics, Digital Corporations

INTRODUCTION

The evolution of corporate activity in the twenty-first century has been marked by a decisive shift from human-centric decision-making to algorithmically driven processes. Artificial intelligence systems now inform, and in some instances autonomously execute, decisions relating to credit scoring, hiring, pricing, supply chain logistics, and even regulatory compliance. While these developments promise efficiency and innovation, they simultaneously complicate the legal architecture governing corporate accountability (Hanlon, 2009).Corporate criminal liability has historically been premised on the ability to attribute wrongful intent and conduct to a juristic entity through human agents. Classical doctrines such as the identification theory locate culpability in the "directing mind and will" of the corporation, typically senior management. However, when decision-making authority is partially or wholly delegated to AI systems, the attribution of intent becomes legally ambiguous. The opacity of machine learning models, often described as "black boxes," further exacerbates this challenge, as neither developers nor corporate executives may fully understand how specific outcomes are generated.This shift raises fundamental questions. Can a corporation be held criminally liable for actions taken by an autonomous system that is neither directly controlled nor fully understood? Does negligence extend to the failure to anticipate emergent behavior in AI systems? And to what extent should liability be recalibrated to account for technological agency?

The urgency of these questions is underscored by real-world instances of algorithmic misconduct. From anti-competitive pricing algorithms to discriminatory hiring tools, corporations have increasingly relied on AI systems that produce legally problematic outcomes. Courts and regulators, however, have struggled to apply existing doctrines coherently in such contexts (An introduction to directors' and officers' liability insurance, n.d.).

CONCEPTUAL FRAMEWORK - CORPORATE CRIME IN THE AGE OF AI

Corporate crime traditionally encompasses unlawful acts committed by a corporation or its representatives for the benefit of the organization. These acts range from financial fraud and environmental violations to antitrust breaches and regulatory non-compliance. The defining feature of corporate crime is the attribution of liability to a legal entity that acts through human agents (Henning, 2014). Artificial intelligence disrupts this paradigm by introducing a non-human decision-making intermediary. AI systems, particularly those based on machine learning, are capable of identifying patterns, adapting to new data, and making decisions without explicit human instructions. Unlike traditional software, which operates on predetermined rules, AI systems evolve over time, making their behavior less predictable.This unpredictability has significant implications for legal responsibility. In conventional corporate crime, liability is often established by demonstrating that a human agent acted with intent or negligence within the scope of their employment. In the AI context, however, harmful outcomes may arise from complex interactions between data inputs, algorithmic design, and environmental variables, rather than deliberate human action.The concept of "algorithmic agency" has thus emerged as a focal point of scholarly debate. While AI systems lack legal personhood, their functional autonomy challenges the binary distinction between human actors and passive tools. Some scholars argue that AI should be treated as an extension of corporate activity, thereby preserving traditional liability frameworks. Others contend that a more nuanced approach is required, one that recognizes the distributed nature of decision-making in AI-driven systems (Purnomo, 2018). Another critical dimension is the opacity of AI systems. Machine learning models, particularly deep learning networks, often operate as black boxes, producing outputs that are difficult to interpret even by experts. This lack of explainability complicates efforts to establish causation and foreseeability, key elements in both criminal and civil liability.Moreover, the deployment of AI systems often involves multiple actors, including developers, data providers, and end-users. This fragmentation of responsibility raises questions about how liability should be apportioned among different authorities. Should liability rest solely with the corporation deploying the AI, or should it be shared with those involved in its creation and maintenance?

These conceptual challenges necessitate a re-examination of foundational legal principles, particularly those relating to mens rea, causation, and organizational fault (Monaghan, 2018).

DOCTRINAL FOUNDATIONS OF CORPORATE CRIMINAL LIABILITY

The identification theory, developed in early English jurisprudence, attributes the actions and mental state of senior corporate officers to the corporation itself. This doctrine was articulated in *Lennard's Carrying Co Ltd v Asiatic Petroleum Co Ltd* ([1915] AC 705), where the House of Lords held that the "directing mind and will" of the corporation could be identified with certain high-ranking individuals. Similarly, in *Tesco Supermarkets Ltd v Nattrass* ([1972] AC 153), the court limited corporate liability to acts of senior management, excluding lower-level employees.While the identification theory provides a clear mechanism for attributing liability, it is ill-suited to modern corporate structures characterized by decentralization and automation. In the context of AI, the doctrine becomes even more problematic. When decisions are made by algorithms rather than identifiable individuals, the notion of a "directing mind" becomes difficult to sustain.

Courts have increasingly recognized these limitations. In *Meridian Global Funds Management Asia Ltd v Securities Commission* ([1995] 2 AC 500), the Privy Council adopted a more flexible approach, emphasizing that rules of attribution should be tailored to the substantive law in question. This decision marked a shift toward a more pragmatic understanding of corporate liability, one that could potentially accommodate

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 3796-3801

technological intermediaries.In jurisdictions such as the United States, corporate criminal liability is often grounded in the doctrine of respondeat superior, which holds corporations liable for the acts of employees committed within the scope of their employment and for the benefit of the organization. In *New York Central & Hudson River Railroad Co v United States* (212 U.S. 481 (1909)), the U.S. Supreme Court affirmed that corporations could be held criminally liable for the actions of their agents.

This doctrine significantly broadens the scope of corporate liability, as it does not require proof of involvement by senior management. However, its application to AI systems is not straightforward. Unlike human employees, AI systems do not possess intent or consciousness, raising questions about whether their actions can be analogized to those of corporate agents (Davies, 2018).

Nevertheless, some scholars argue that AI systems should be treated as functional equivalents of employees, thereby extending vicarious liability principles to algorithmic conduct. This approach, however, risks oversimplifying the unique characteristics of AI and may lead to over- or under-inclusive liability outcomes.

Aggregation Doctrine and Collective Knowledge

The aggregation doctrine allows courts to combine the knowledge of multiple employees to establish corporate intent. This approach recognizes that corporate decision-making is often distributed across different individuals, none of whom may possess complete knowledge of the wrongdoing (Hooper, 2018).

In *United States v Bank of New England* (821 F.2d 844 (1st Cir. 1987)), the court held that a corporation's knowledge could be aggregated from the collective knowledge of its employees. This doctrine is particularly relevant in the AI context, where decision-making involves multiple layers of human and technological inputs.

However, aggregation also raises concerns about fairness and proportionality. Attributing collective knowledge to a corporation may result in liability even when no single individual acted with culpable intent. In the case of AI systems, where outcomes may emerge from complex data interactions, the application of aggregation becomes even more contentious.

Corporate Culture and Organizational Fault

In response to the limitations of traditional doctrines, some jurisdictions have adopted a "corporate culture" approach to liability. This model, reflected in statutes such as the Australian Criminal Code, focuses on the organization's policies, practices, and culture in determining fault.

The corporate culture model is particularly relevant in the AI context, as it emphasizes systemic factors rather than individual actions. For example, a corporation that fails to implement adequate oversight mechanisms for its AI systems may be deemed to have fostered a culture of non-compliance (Hurley, 2018). This approach aligns with contemporary governance frameworks that prioritize risk management, compliance, and ethical standards. However, it also requires courts to engage in complex assessments of organizational behavior, which may be difficult to operationalize in practice.

AI-INDUCED MISCONDUCT: NATURE, TYPOLOGIES, AND LEGAL CHALLENGES

The integration of artificial intelligence into corporate operations has given rise to a new category of misconduct that is qualitatively distinct from traditional corporate crime. Unlike conventional wrongdoing, which is typically the result of deliberate human action or negligence, AI-induced misconduct often emerges from complex, data-driven processes that may not be fully understood by those deploying the systems. This creates a significant challenge for legal frameworks that rely on notions of intent, foreseeability, and direct causation.

AI-induced misconduct can broadly be categorized into three forms, which are algorithmic collusion, discriminatory decision-making, and compliance failures. Each of these forms raises unique legal and regulatory concerns, particularly in relation to attribution of liability and the adequacy of existing compliance mechanisms (Monaghan, 2018).

Algorithmic collusion represents one of the most significant risks associated with AI deployment in competitive markets. Pricing algorithms, designed to optimize profits, may independently learn to coordinate with competitors' algorithms, resulting in tacit collusion without any explicit agreement between firms. This phenomenon challenges the traditional foundations of competition law, which are premised on the existence of an agreement or concerted practice.

Discriminatory decision-making is another prominent area of concern. AI systems used in hiring, lending, and insurance have been shown to produce biased outcomes, often reflecting historical inequalities embedded in training data. In such cases, the corporation may not have intended to discriminate, yet the outcomes can still violate anti-discrimination laws.

Compliance failures, particularly in highly regulated sectors such as finance and healthcare, further illustrate the risks of AI deployment. Automated systems used for fraud detection, risk assessment, or regulatory reporting may fail to identify violations or may themselves produce inaccurate outputs, leading to breaches of legal obligations (Glover, 2018).

These forms of misconduct underscore the need for a re-evaluation of legal standards governing corporate liability, particularly in relation to foreseeability and due diligence.

ALGORITHMIC COLLUSION AND COMPETITION LAW CHALLENGES

One of the most widely discussed manifestations of AI-induced misconduct is algorithmic collusion. Unlike traditional cartels, which involve explicit agreements between competitors, algorithmic collusion may arise spontaneously through the interaction of pricing algorithms. These systems, trained to maximize profits, can learn to avoid price competition and maintain supra-competitive prices (Palmer, 2018).

A seminal case illustrating the use of algorithms in anti-competitive conduct is *United States v Topkins* (No. 3:15-cr-00201 (N.D. Cal. 2015)), where the defendant used pricing algorithms to coordinate prices of posters sold on an online marketplace. Although this case involved explicit collusion facilitated by algorithms, it highlights the potential for technology to enable anti-competitive behavior (*United States v Topkins* (2015)).More complex scenarios arise when collusion is not explicitly programmed but emerges from machine learning processes. In such cases, establishing an "agreement" becomes difficult, as required under competition law frameworks such as Section 1 of the Sherman Act in the United States or Article 101 of the Treaty on the Functioning of the European Union (Monaghan, 2018).

The European Commission has acknowledged this challenge, noting that algorithmic systems may facilitate collusion even in the absence of direct human involvement. However, existing legal frameworks have struggled to adapt, as they are not designed to address autonomous coordination between non-human actors.From a liability perspective, the key question is whether corporations can be held responsible for outcomes that were neither intended nor foreseeable. Some scholars argue for the application of strict liability in such cases, emphasizing the need to deter the deployment of potentially harmful technologies. Others advocate for a negligence-based approach, focusing on whether the corporation exercised adequate oversight and risk management (Flores, 2018). The absence of clear legal standards in this area creates uncertainty for both regulators and corporations, underscoring the need for more explicit guidance on the use of AI in competitive markets.

DISCRIMINATORY ALGORITHMS AND CORPORATE ACCOUNTABILITY

AI-driven discrimination represents another critical dimension of corporate misconduct. Unlike traditional forms of discrimination, which are often overt and intentional, algorithmic bias is typically indirect and embedded within data or model design. This makes it more difficult to detect and address (Collins, 2018).

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 3796-3801

A notable example is *State of Wisconsin v Loomis* (881 N.W.2d 749 (Wis. 2016)), where the use of a risk assessment algorithm in sentencing raised concerns about transparency and bias. Although the court upheld the use of the tool, it acknowledged the limitations of proprietary algorithms and the potential for discriminatory outcomes (State v Loomis (2016)).

In the corporate context, similar issues have arisen in hiring and lending practices. In *Griggs v Duke Power Co* (401 U.S. 424 (1971)), the U.S. Supreme Court established the principle of disparate impact, holding that practices that are neutral on their face but discriminatory in effect can violate anti-discrimination laws. This doctrine is particularly relevant to AI systems, which may produce biased outcomes even in the absence of discriminatory intent (Griggs v Duke Power Co (1971)).

More recently, regulatory scrutiny has increased. The Equal Employment Opportunity Commission in the United States and data protection authorities in the European Union have issued guidance on the use of AI in employment decisions, emphasizing the need for transparency, fairness, and accountability (Purnomo, 2018).

In the European context, the General Data Protection Regulation (GDPR) provides a framework for addressing algorithmic decision-making, including the right to an explanation under Article 22. However, the practical implementation of this right remains contested, particularly in relation to complex machine learning models (Tsai, 2014).

In India, while there is no comprehensive AI-specific legislation, existing constitutional and statutory provisions may be invoked to address algorithmic discrimination. The right to equality under Article 14 of the Constitution, as interpreted in *E.P. Royappa v State of Tamil Nadu* ((1974) 4 SCC 3), emphasizes non-arbitrariness as a core principle, which could extend to automated decision-making systems.

These developments indicate a growing recognition of the risks posed by AI-driven discrimination, but also highlight the limitations of existing legal frameworks in addressing such risks effectively.

AI IN FINANCIAL MISCONDUCT AND COMPLIANCE FAILURES

The financial sector has been at the forefront of AI adoption, particularly in areas such as fraud detection, credit scoring, and algorithmic trading. While these technologies offer significant benefits, they also introduce new risks of misconduct and regulatory breaches (Clinard, 2017). A prominent example is the "flash crash" of 2010, where algorithmic trading systems contributed to a rapid and severe market decline. In *Commodity Futures Trading Commission v Navinder Singh Sarao* (No. 15 CR 75 (N.D. Ill. 2015)), the defendant was accused of using automated trading algorithms to manipulate the market, highlighting the potential for AI systems to facilitate financial misconduct (CFTC v Sarao (2015)).More broadly, the use of AI in compliance functions raises questions about the adequacy of automated systems in meeting regulatory requirements. Financial institutions increasingly rely on AI for anti-money laundering (AML) and know-your-customer (KYC) processes. However, failures in these systems can lead to significant legal consequences, including fines and reputational damage (Bufton, 2025). Regulators have begun to address these risks through guidance and supervisory frameworks. For instance, the Basel Committee on Banking Supervision has emphasized the importance of model risk management, requiring institutions to validate and monitor their AI systems continuously.In India, regulatory bodies such as the Reserve Bank of India have issued guidelines on digital lending and fintech operations, indirectly addressing the use of AI in financial services. However, the absence of a comprehensive regulatory framework for AI creates gaps in oversight, particularly in relation to accountability and transparency (Hanlon, 2009).

The reliance on AI in compliance functions also raises a paradox, systems designed to ensure compliance may themselves become sources of non-compliance. This underscores the need for robust governance frameworks that integrate human oversight with technological capabilities.

EMERGING JUDICIAL AND REGULATORY RESPONSES

Courts and regulators across jurisdictions have begun to grapple with the challenges posed by AI-induced misconduct, albeit in a fragmented and evolving manner. While no comprehensive legal framework has yet emerged, several trends can be identified.

First, there is a growing emphasis on due diligence and risk management. Corporations are increasingly expected to assess the risks associated with AI deployment and to implement appropriate safeguards. Failure to do so may result in liability, even in the absence of intent (Sari,, 2023).

Second, there is a shift toward greater transparency and explainability. Regulators are demanding that corporations provide meaningful explanations for algorithmic decisions, particularly in high-stakes contexts such as employment and finance. Third, there is an increasing recognition of the need for interdisciplinary approaches to regulation. Legal frameworks must be complemented by technical standards, ethical guidelines, and industry best practices. The European Union has taken a leading role in this area through its proposed Artificial Intelligence Act, which adopts a risk-based approach to regulation. High-risk AI systems are subject to stringent requirements, including conformity assessments, documentation, and human oversight (Hughes, 2025). In US, regulatory approaches remain more fragmented, with sector-specific guidelines and enforcement actions shaping the landscape. In India, policy discussions are ongoing, with initiatives such as the National Strategy for Artificial Intelligence highlighting the need for responsible AI governance. Despite these developments, significant gaps remain. Existing frameworks are often reactive rather than proactive, addressing harms after they occur rather than preventing them. Moreover, the global nature of AI deployment complicates regulatory efforts, as corporations operate across multiple jurisdictions with differing legal standards (Brown, 2001).

RECONFIGURING MENS REA IN THE AGE OF ARTIFICIAL INTELLIGENCE

One of the most profound challenges posed by artificial intelligence to corporate criminal liability lies in the concept of *mens rea*, or the mental element of a crime. Traditional criminal law requires proof of intent, knowledge, recklessness, or negligence. These categories presuppose human cognition and volition, making their application to AI-driven conduct inherently problematic (Brown, 2000).

Corporations, as artificial legal persons, have always required doctrinal mechanisms to attribute mens rea through human agents. However, when decision-making is delegated to AI systems that operate autonomously, the connection between human intent and corporate action becomes attenuated. In such scenarios, harmful outcomes may arise without any individual possessing the requisite mental state.

This raises a critical question, can mens rea be reconstructed in a way that accommodates technological agency? One approach is to shift the focus from subjective intent to objective foreseeability. Under this model, a corporation may be held liable if it was reasonably foreseeable that the deployment of an AI system could result in harm. This aligns with negligence-based standards, which emphasize the failure to exercise due care (Zulkarnain, 2021). Judicial reasoning in cases such as *R v G* ([2003] UKHL 50) has underscored the importance of subjective recklessness in criminal law, requiring that the defendant be aware of a risk and unreasonably take it. Translating this standard to AI contexts, however, is difficult. Corporate actors may not fully understand the risks associated with complex machine learning systems, raising questions about what constitutes "awareness."An alternative approach is to adopt a form of "constructive knowledge," whereby corporations are deemed to possess knowledge of risks that they ought reasonably to have identified through due diligence. This approach is consistent with regulatory trends emphasizing risk assessment and compliance obligations (Hanlon, 2009).

Ultimately, the concept of mens rea in the AI context may need to evolve from a focus on individual culpability to an emphasis on organizational responsibility. This shift reflects the reality that AI-induced misconduct often arises from systemic failures rather than isolated acts of wrongdoing.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 3796-3801

ATTRIBUTION CHALLENGES IN AI-DRIVEN CORPORATE STRUCTURES

Attribution remains a central issue in determining corporate liability. Traditional doctrines rely on identifying a human agent whose actions and mental state can be imputed to the corporation. However, AI systems complicate this process by introducing multiple layers of decision-making and diffused responsibility (Hanlon, 2009).

The problem of attribution is particularly acute in cases involving complex AI ecosystems. A single AI system may be developed by one entity, trained on data provided by another, and deployed by a third. When misconduct occurs, determining which party is responsible becomes a challenging legal exercise.

Judicial approaches to attribution have evolved over time to address similar complexities. In *Meridian Global Funds Management Asia Ltd v Securities Commission* ([1995] 2 AC 500), the Privy Council emphasized that rules of attribution should be tailored to the purpose of the relevant legal provision. This flexible approach provides a potential pathway for addressing AI-related cases, allowing courts to adapt attribution principles to new technological contexts.

However, flexibility alone may not be sufficient. The opacity of AI systems makes it difficult to establish causation, as the link between input data, algorithmic processing, and output decisions may not be readily apparent. This complicates the application of legal standards that require proof of a causal connection between conduct and harm (Militello, 2024).

Moreover, the diffusion of responsibility within corporations further exacerbates attribution challenges. In large organizations, decisions relating to AI deployment may involve multiple departments, including data science teams, compliance officers, and senior management. Each of these actors may contribute to the overall outcome, yet none may bear sole responsibility.

The aggregation doctrine, as applied in *United States v Bank of New England* (821 F.2d 844 (1st Cir. 1987)), offers one solution by combining the knowledge of multiple actors. However, its application to AI systems raises concerns about over-extension of liability, particularly when outcomes are not directly attributable to any individual's conduct.

These challenges suggest the need for new attribution models that account for the distributed and autonomous nature of AI systems. Such models must balance the goals of accountability and fairness, ensuring that liability is neither unduly diluted nor excessively broad.

CORPORATE GOVERNANCE FAILURES AND AI RISK MANAGEMENT

The rise of AI has exposed significant gaps in corporate governance frameworks, particularly in relation to risk management and oversight. Traditional governance structures are designed to monitor human decision-making, relying on internal controls, audits, and compliance mechanisms. However, these tools are often inadequate for managing the risks associated with AI systems

One of the key governance challenges is the lack of technical expertise at the board level. Directors may not possess the knowledge required to understand the functioning and risks of AI systems, leading to inadequate oversight. This issue is compounded by the rapid pace of technological change, which makes it difficult for governance frameworks to keep up.The importance of effective governance is highlighted in cases such as *In re Caremark International Inc Derivative Litigation* (698 A.2d 959 (Del. Ch. 1996)), where the court emphasized the duty of directors to ensure that adequate information and reporting systems are in place. Failure to do so may constitute a breach of fiduciary duty (In re Caremark (1996)).In the AI context, this duty extends to the implementation of robust monitoring systems for algorithmic decision-making. Corporations must ensure that AI systems are subject to continuous evaluation, including validation, testing, and auditing. The absence of such measures may be construed as negligence or even recklessness.Another governance challenge is the integration of ethical considerations into corporate decision-making. AI systems often operate based on optimization objectives, such as maximizing profit or efficiency, which may conflict with legal and ethical standards. Without appropriate safeguards, these systems may produce outcomes that are legally permissible but ethically questionable (Tarasiuk, 2023). The concept of "ethical by design" has gained prominence as a means of addressing this issue. This approach involves embedding ethical principles into the design and deployment of AI systems, ensuring that they align with societal values and legal requirements.However, the implementation of ethical frameworks requires more than technical solutions. It necessitates a cultural shift within organizations, emphasizing accountability, transparency, and responsibility. This aligns with the corporate culture model of liability, which focuses on systemic factors rather than individual actions.

THE CASE FOR ADAPTIVE MANAGEMENT POLICIES

Given the limitations of existing governance frameworks, there is a pressing need for adaptive management policies that can respond to the dynamic nature of AI systems. Unlike traditional compliance mechanisms, which are often static and rule-based, adaptive policies emphasize flexibility, continuous learning, and responsiveness.

Adaptive management involves several key components. First, it requires ongoing risk assessment, recognizing that the behavior of AI systems may evolve over time. Corporations must therefore implement mechanisms for continuous monitoring and evaluation, rather than relying on one-time assessments.Second, adaptive management emphasizes the importance of feedback loops. Information about the performance and impact of AI systems should be used to inform decision-making and improve system design. This iterative approach allows organizations to respond to emerging risks and challenges.Third, human oversight remains a critical element of adaptive management. While AI systems can operate autonomously, human intervention is necessary to ensure accountability and to address unforeseen issues. The concept of "human-in-the-loop" governance has emerged as a key principle in this regard, ensuring that critical decisions are subject to human review.

The importance of adaptive approaches is reflected in regulatory developments. For example, the European Union's proposed AI framework emphasizes lifecycle management, requiring continuous monitoring and updating of high-risk AI systems. Similarly, international organizations such as the OECD have advocated for principles of responsible AI, including accountability, transparency, and robustness.

In the Indian context, the need for adaptive management is particularly acute given the rapid growth of digital platforms and AI-driven services. While regulatory frameworks are still evolving, corporations must take proactive steps to address AI-related risks, including the development of internal policies and governance structures.Ultimately, adaptive management represents a shift from reactive to proactive compliance. Rather than responding to misconduct after it occurs, organizations must anticipate and mitigate risks in advance. This approach not only enhances legal compliance but also promotes trust and sustainability in the use of AI technologies.

TOWARD A HYBRID LIABILITY FRAMEWORK

The challenges discussed in this paper suggest that no single doctrinal approach is sufficient to address AI-induced misconduct. Instead, a hybrid liability framework may be required, combining elements of strict liability, negligence, and organizational fault.Strict liability may be appropriate in high-risk contexts, where the potential for harm is significant and difficult to predict. By imposing liability regardless of intent, this approach creates strong incentives for corporations to exercise caution in deploying AI systems.At the same time, negligence-based standards remain important in assessing whether corporations have fulfilled their duty of care. This includes evaluating the adequacy of risk assessments, oversight mechanisms, and compliance programs.The corporate culture model provides an additional layer of analysis, focusing on systemic factors and organizational practices. By examining the broader context in which AI systems are deployed, this approach captures the complexity of modern corporate structures.A hybrid framework thus offers a more nuanced and flexible approach to liability, accommodating the unique challenges posed by AI while preserving the core principles of accountability and deterrence.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 3796-3801

CONCLUSION

The transition from traditional corporate decision-making structures to AI-driven "black box" systems marks a profound shift in the nature of corporate conduct and, consequently, corporate criminal liability. As this paper has demonstrated, existing legal doctrines, whether grounded in identification theory, vicarious liability, or aggregation, are increasingly strained when applied to autonomous, opaque, and adaptive technologies. The central challenge lies not merely in technological complexity, but in the conceptual mismatch between human-centric legal principles and machine-mediated decision-making.

AI-induced misconduct, whether in the form of algorithmic collusion, discriminatory outcomes, or compliance failures, exposes the inadequacy of frameworks that rely heavily on intent, direct control, and linear causation. The diffusion of responsibility across developers, deployers, and data ecosystems further complicates attribution, while the opacity of machine learning models undermines transparency and evidentiary clarity. In such an environment, the traditional anchors of corporate liability, mens rea and identifiable agency, lose their determinacy.

This paper has argued that the solution does not lie in abandoning established principles, but in recalibrating them. A shift toward organizational responsibility, grounded in foreseeability, due diligence, and systemic oversight, offers a more viable path forward. The emergence of corporate culture models and negligence-based standards reflects this transition, emphasizing that liability must attach not only to wrongful acts, but to the conditions that enable them. In the AI context, this includes failures in design, deployment, monitoring, and governance.

Equally is the need for adaptive management policies within corporations. Static compliance mechanisms are ill-suited to technologies that evolve over time. Instead, organizations must adopt continuous auditing, algorithmic transparency, and human-in-the-loop oversight to ensure that AI systems remain aligned with legal and ethical norms. This proactive approach transforms compliance from a reactive obligation into an integral component of corporate strategy.

From a regulatory perspective, a hybrid liability framework, combining elements of strict liability, negligence, and organizational fault, appears most appropriate. Such a model balances the need for deterrence with considerations of fairness, ensuring that corporations cannot evade accountability by invoking technological complexity, while also recognizing the limits of human foresight.

Ultimately, as corporations move from boardrooms to black boxes, the law must evolve in tandem. The legitimacy of corporate activity in the age of artificial intelligence will depend on the ability of legal systems to ensure that innovation does not come at the cost of accountability. The future of corporate criminal liability, therefore, lies in its capacity to adapt, preserving its foundational principles while embracing the realities of a technologically mediated world.

REFERENCES

- Hanlon, J. P. (2009). Principles of criminal liability for corporate misconduct. In *Punishing corporate crime* (pp. 25–39). Oxford University Press. https://doi.org/10.1093/oso/9780195386790.003.0003
- An introduction to directors' and officers' liability insurance. (n.d.). In *Ensuring corporate misconduct* (pp. 42–56). University of Chicago Press. https://doi.org/10.7208/chicago/9780226035079.003.0004
- Henning, P. J. (2014). A new crime for corporate misconduct? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2379586
- Purnomo, H., & Santiago, F. (2018). The corporate crime liability for environmental pollution. In *Proceedings of the 2018 International Conference on Energy and Mining Law (ICEML 2018)*. Atlantis Press. https://doi.org/10.2991/iceml-18.2018.23
- Monaghan, C. (2018). A critical commentary on the Fraud Act 2006. In *Financial crime and corporate misconduct* (pp. 1–13). Routledge. https://doi.org/10.4324/9781315150642-1
- Davies, B. (2018). Do we need a failure to prevent fraud offence? In *Financial crime and corporate misconduct* (pp. 133–143). Routledge. https://doi.org/10.4324/9781315150642-10
- Hooper, T. (2018). A judge's perspective of the impact of the Fraud Act 2006. In *Financial crime and corporate misconduct* (pp. 144–158). Routledge. https://doi.org/10.4324/9781315150642-11
- Hurley, S. (2018). The fraudster at work. In *Financial crime and corporate misconduct* (pp. 159–175). Routledge. https://doi.org/10.4324/9781315150642-12
- Monaghan, N. (2018). Who should try 'complex fraud trials'? In *Financial crime and corporate misconduct* (pp. 176–191). Routledge. https://doi.org/10.4324/9781315150642-13
- Glover, R. (2018). Good character directions. In *Financial crime and corporate misconduct* (pp. 192–206). Routledge. https://doi.org/10.4324/9781315150642-14
- Palmer, A. (2018). The Fraud Act's 10th anniversary. In *Financial crime and corporate misconduct* (pp. 14–31). Routledge. https://doi.org/10.4324/9781315150642-2
- Monaghan, C. (2018). An empirical review of the use of the Fraud Act 2006 and other criminal offences within the school application system. In *Financial crime and corporate misconduct* (pp. 32–47). Routledge. https://doi.org/10.4324/9781315150642-3
- Flores Elizondo, C. J., Lord, N., & Spencer, J. (2018). Food fraud and the Fraud Act 2006. In *Financial crime and corporate misconduct* (pp. 48–62). Routledge. https://doi.org/10.4324/9781315150642-4
- Collins, C., & McGuirk, N. (2018). Fraud in the twenty-first century. In *Financial crime and corporate misconduct* (pp. 63–78). Routledge. https://doi.org/10.4324/9781315150642-5
- Purnomo, H., & Santiago, F. (2018). The corporate crime liability for environmental pollution. In *Proceedings of the 2018 International Conference on Energy and Mining Law (ICEML 2018)*. Atlantis Press. https://doi.org/10.2991/iceml-18.2018.23
- Tsai, H.-C. (2014). *Corporate crime and corporate liability* (Doctoral dissertation). https://ndltd.ncl.edu.tw/handle/71749624757227036487
- Clinard, M. B., Yeager, P. C., & Clinard, R. B. (2017). Corporate executives and criminal liability. In *Corporate crime* (pp. 272–298). Routledge. https://doi.org/10.4324/9781315080314-12
- Bufton, G. (2025). Corporate criminal liability. In *Contemporary economic crime* (1st ed., pp. 129–137). Routledge. https://doi.org/10.4324/9781003324843-15
- Hanlon, J. P. (2009). Criminal statutory liability and interpretation. In *Punishing corporate crime* (pp. 47–64). Oxford University Press. https://doi.org/10.1093/oso/9780195386790.003.0006
- Sari, N. K. A. (2023). Criminal liability for corporate crime in Indonesia. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam, 5*(1), 867–874. https://doi.org/10.37680/almanhaj.v5i1.2687
- Hughes, R. C. (2025). Corporate criminal liability and the purposes of punishment. In *Corporate crime* (1st ed., pp. 18–37). Routledge. https://doi.org/10.4324/9781003088455-3
- Brown, D. K. (2001). Street crime, corporate crime, and the contingency of criminal liability. *University of Pennsylvania Law Review, 149*(5), 1295–1360. https://doi.org/10.2307/3312963
- Brown, D. K. (2000). Street crime, corporate crime and the contingency of criminal liability. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.253063
- Zulkarnain, Z., Nurjaya, I. N., Sugiri, B., & Navianto, I. (2021). Corporate crime and corporate criminal liability in Indonesia positive law. *ENDLESS: International Journal of Future Studies, 4*(2), 20–30. https://doi.org/10.54783/endless.v4i2.58
- Hanlon, J. P. (2009). Individual criminal liability related to the corporation. In *Punishing corporate crime* (pp. 41–46). Oxford University Press. https://doi.org/10.1093/oso/9780195386790.003.0005

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 3796-3801

- Hanlon, J. P. (2009). Principles of criminal liability for corporate misconduct. In *Punishing corporate crime* (pp. 25–39). Oxford University Press. https://doi.org/10.1093/oso/9780195386790.003.0003
- Militello, V. (2024). Corporate criminal liability. In *Elgar encyclopedia of crime and criminal justice*. Edward Elgar Publishing. https://doi.org/10.4337/9781789902990.corporate.criminal.liability
- Handayani, E. P., & Hasyim, M. W. (2018). Corporate crime liability towards environmental law in Indonesia. *Indonesian Journal of Law and Economics Review, 2*(1). https://doi.org/10.21070/ijler.2018.v2.686
- Tarasiuk, A., Prokofieva-Yanchylenko, D., Lutsenko, Y., Danylevskyi, A., & Makarenko, T. (2023). Corporate liability and white-collar crime: Comparative review. *Cuestiones Políticas, 41*(78), 523–540. https://doi.org/10.46398/cuestpol.4178.36
- Norrie, A. (n.d.). Strict and corporate liability. In *Crime, reason and history* (pp. 102–134). Cambridge University Press. https://doi.org/10.1017/cbo9781139031851.011
- Hellman, J. (2014). The fifth crime under international criminal law: Ecocide? In *Regulating corporate criminal liability* (pp. 273–280). Springer International Publishing. https://doi.org/10.1007/978-3-319-05993-8_22
- Laufer, W. S. (2014). Where is the moral indignation over corporate crime? In *Regulating corporate criminal liability* (pp. 19–31). Springer International Publishing. https://doi.org/10.1007/978-3-319-05993-8_3
- Corporate criminal liability: From immunity to culpability. (2014). In *Corporate crime under attack* (pp. 73–108). Routledge. https://doi.org/10.4324/9781315721996-8
- Putra, P. S. (2024). The corporate liability as perpetrator of environmental pollution crime. *JURNAL AKTA, 11*(2), 462. https://doi.org/10.30659/akta.v11i2.37463
- Gobert, J. (n.d.). The evolving legal test of corporate criminal liability. In *Corporate and white-collar crime* (pp. 61–80). SAGE Publications Ltd. https://doi.org/10.4135/9781446214619.n4
- Horder, J. (2025). Corporate criminal liability under the Economic Crime and Corporate Transparency Act 2023. *Legal Studies*, 1–16. https://doi.org/10.1017/lst.2024.46
- Suartha, I. D. M., & Ivory, J. (2024). Corporate crime liability: Beyond rule reform on Indonesia criminal policy. *Focus Journal Law Review, 4*(2). https://doi.org/10.62795/fjl.v4i2.281
- Shidarta. (2019). Extensive interpretation of corporate liability in the crime of illegal fishing in Indonesia. In *Proceedings of the International Conference on Maritime and Archipelago (ICoMA 2018)*. Atlantis Press. https://doi.org/10.2991/icoma-18.2019.51
- Kemp, G. (2024). Institutional and substantive responses to economic and transnational organised crime. In *Corporate criminal liability and sanctions* (1st ed., pp. 127–139). Routledge. https://doi.org/10.4324/9781003324829-10