Page 742 - 755 **DOI:** *https://doij.org/10.10000/IJLMH.1111316*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 1

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/

Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Corporate Law in the Digital Age: Emerging Legal Issues in AI, Data Protection, and FinTech

MOHIT KHARB[1] AND PARTHA PRATIM MITRA[2]

ABSTRACT

The regulatory landscape and corporate governance have been drastically changed by the rapid uptake of digital technology. Artificial intelligence, data-driven business models, and financial technology have all improved market competitiveness and operational efficiency while also posing new legal and regulatory issues. The application of artificial intelligence, the enforcement of data protection laws, and the growth of FinTech ecosystems all give rise to new corporation law concerns that are critically examined in this essay. Concerns like data privacy, algorithmic transparency, corporate responsibility, cybersecurity threats, and regulatory compliance receive special emphasis. The analysis finds regulatory loopholes that could jeopardize stakeholder protection and evaluates how well the current legal frameworks handle these issues. It emphasizes even more how important it is to have flexible, technology-neutral legal frameworks that support innovation while defending moral principles, consumer interests, and systemic stability. By providing insights into the changing role of company law in regulating digital transition, the study advances current legal scholarship.

Keywords: *Corporate Law, Artificial Intelligence, Data Protection, FinTech, Digital Governance, Regulatory Frameworks*

I. INTRODUCTION

The rapid advancement of digital technologies particularly artificial intelligence (AI), data-centric business models, and financial technology (FinTech) is not merely reshaping commercial practice, but fundamentally transforming the legal landscape that governs corporate conduct. Modern corporate law, traditionally shaped around human decision-making and stable organisational structures, is now being tested by technologies capable of autonomous action, continuous data processing, and cross-border financial intermediation. These developments raise pressing questions about corporate accountability, governance, and the adequacy of existing regulation to address emerging risks (Andreevich and Feyzrakhmanova, 2021; Allah

[1] Author is a Student at Faculty of Law, Vivekananda Global University, Jaipur, Rajasthan, India.
[2] Author is the Dean and Professor at Faculty of Law, Vivekananda Global University, Jaipur, Rajasthan, India.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Rakha, 2023). A central tension in this transformation lies in reconciling **innovation with legal responsibility**. AI systems entrusted with corporate decision-making can improve efficiency and predictive insight, yet they also introduce potential legal liabilities from algorithmic bias to non-transparent internal governance processes. This is evident in comparative legal analyses exploring liability frameworks for businesses deploying AI services across jurisdictions, which highlight the difficulty of assigning legal responsibility where autonomous or semi-autonomous systems cause harm (Mirishli, 2025).

Equally significant is the challenge of **data protection in a digital economy**. Personal data has become a core corporate resource, central to everything from customer profiling to credit scoring and automated compliance systems. The integration of AI into these processes intensifies existing concerns about privacy and regulatory compliance. Data protection regimes such as the European Unions GDPR exemplify how legal frameworks attempt to protect individual privacy, yet companies operating in multiple jurisdictions face fragmented regulatory landscapes that complicate compliance (McIlroy and Phillis, 2025; Aggarwal, 2023) . In this context, scholars argue that corporate governance must evolve to recognise digital stakeholders including data subjects and embed principles of transparency and accountability within AI-driven systems (Laptev and Feyzrakhmanova, 2021; corporate digital responsibility frameworks) .

FinTech further complicates the regulatory environment by accelerating the integration of digital innovation into core financial services. Products such as smart contracts, digital currencies, and automated credit scoring challenge traditional financial regulation and demand new legal tools to balance market efficiency with consumer protection and systemic stability. Comparative regulatory studies demonstrate that both developed and developing economies struggle to keep pace with FinTechs rapid evolution, resulting in gaps that may expose firms to legal uncertainties and consumers to financial risks (Vijayagopal *et al*., 2024).

Within this milieu, there is growing recognition of **the need for adaptive legal frameworks** capable of responding to both the opportunities and risks arising from digital transformation. For instance, regulatory proposals such as the EUs Artificial Intelligence Act seek to harmonise AI governance across high-risk sectors, including finance, by imposing requirements for explainability, fairness, and safety (Cornelius, 2025). Without such evolving frameworks, corporations may face conflicts between innovation incentives and legal compliance, potentially undermining corporate legitimacy and public trust.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The rise of AI in corporate and financial domains also intersects with deeper philosophical and ethical questions. Legal scholarship has begun to explore the notion of **information fiduciaries** obligations that digital platforms and organisations owe to users whose data and decisions they influence reframing traditional fiduciary duties for the digital age (Balkin, 2014) . This reflects a broader trend: legal systems are striving not just to regulate technology, but to integrate ethical considerations into corporate conduct and governance in a digitally mediated world.

Corporate law in the digital age must grapple with a triad of emerging legal issues: the governance and accountability of AI applications; the protection of personal data as a corporate resource; and the regulatory challenges introduced by FinTech innovations. This research review sets out to examine these issues systematically, drawing on comparative legal studies, regulatory analyses, and evolving doctrinal scholarship to illuminate the contours of corporate laws digital transformation.

II. ARTIFICIAL INTELLIGENCE AND CORPORATE GOVERNANCE

Artificial Intelligence (AI) has emerged as a transformative force in corporate governance, fundamentally reshaping how boards make decisions, monitor compliance, and manage risks (Kalkan, 2024). Traditionally, corporate governance revolved around human judgement, fiduciary duties, and manual compliance checks. However, with the increasing adoption of AI systems in executive decision-making and operational workflows, legal and ethical questions have come to the fore requiring reevaluation of existing corporate law frameworks. AIs ability to analyze large datasets, generate predictive insights, and automate routine tasks presents both opportunities and legal challenges for corporate governance.

- **Enhancing Decision-Making and Governance Efficiency**

AI technologies support data-driven decision-making by integrating complex analytical capabilities that far exceed human capacities (Vineeta and Rajoria, 2025). For example, AI can forecast performance trends and risk anomalies, aiding boards in strategic planning and compliance monitoring in real time. Such advanced predictive analytics contribute to enhanced transparency and accountability in corporate structures (Vineeta and Rajoria, 2025).Despite these advantages, reliance on AI raises fundamental questions about legal accountability. While algorithms may improve objectivity, they also risk creating opacity ("black-box" problem) where stakeholders cannot fully understand or justify AI-generated recommendations or outcomes (Ustahaliloğlu, 2025; Kalkan, 2024). This opacity can undermine the validity of decisions and complicate legal assessment when those decisions result in losses or regulatory breaches.

- **Legal and Regulatory Challenges**

a) **Accountability and Liability**

AIs use in corporate governance complicates traditional legal accountability. Directors and officers remain legally responsible for decisions, even if made or influenced by AI (Mondaq, 2025). In India, statutory duties require personal oversight, preventing liability evasion through AI delegation. Globally, cases like U.S. "AI washing" lawsuits show companies can face legal risk for misrepresenting AI capabilities (Reuters News, 2025).

b) **Algorithmic Opacity and Fiduciary Duty**

AIs complex, opaque algorithms challenge the "informed" aspect of fiduciary duties. Directors relying on AI may struggle to justify decisions under corporate law if they cannot explain the AIs reasoning (Ustahaliloğlu, 2025; Springer, 2025).

c) **Data Privacy and Protection**

AI depends on large-scale data, raising compliance issues under privacy laws. Indias DPDP Act, 2023, and the EU GDPR mandate strict rules on consent, processing, and cross-border transfers, requiring robust data governance to avoid penalties and reputational damage (Mondaq, 2025). Figure 1 illustrates the legal and regulatory challenges of integrating AI into corporate governance.

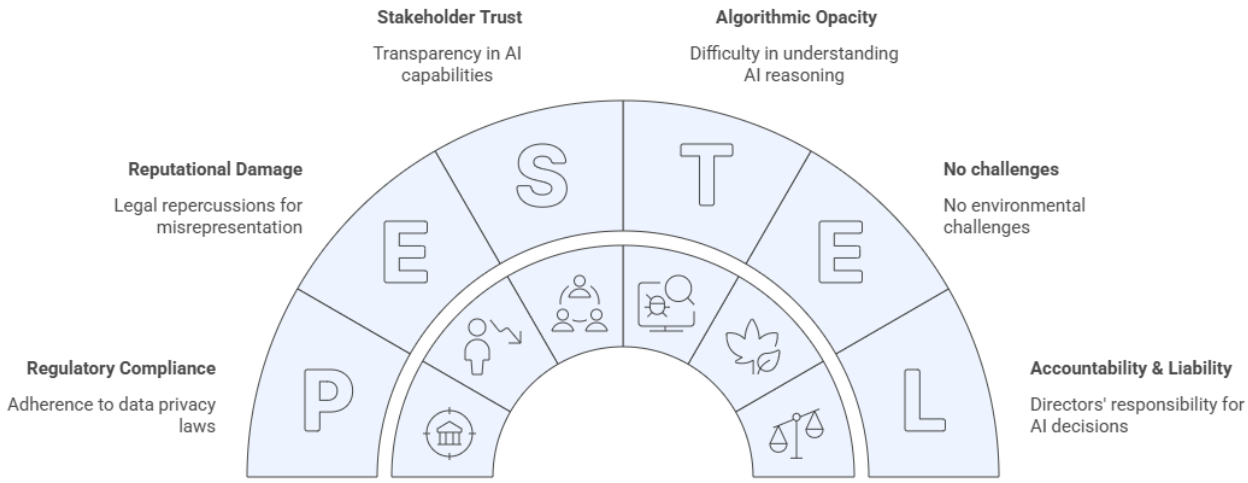

Fig 1: AI in Corporate Governance: Legal and Regulatory Challenges

- **Governance Frameworks and Best Practices**

To address the multifaceted challenges posed by AI, corporations and regulators are increasingly advocating for structured governance frameworks. Dynamic frameworks that integrate continuous human oversight, algorithmic auditing, and risk assessment protocols can

mitigate legal and ethical risks (Ganesh *et al*., 2025). For example, periodic algorithm audits and compliance checks help ensure that AI systems adhere to legal norms and ethical standards. Boards also need to invest in technical literacy and expertise to understand AI capabilities and limitations. Enhanced board competencies can enable more effective oversight of complex AI systems and ensure alignment with corporate strategy and compliance obligations. Furthermore, emerging discourse suggests reconfiguring governance models to explicitly define roles and responsibilities for AI oversight within corporate structures. Such models might delineate clear escalation paths, documentation requirements, and accountability matrices to manage AI systems responsibly.

III. LEGAL CHALLENGES AND LIABILITY ISSUES IN AI IMPLEMENTATION

The integration of artificial intelligence (AI) across corporate systems has driven unprecedented efficiency and innovation but has simultaneously escalated complex legal challenges concerning accountability and liability. As AI systems assume increasingly autonomous roles in decision-making, traditional legal frameworks, which are grounded in human agency and foreseeability, struggle to address the unique risks posed by machine learning algorithms, opaque decision processes, and adaptive behaviors that evolve post-deployment. Central to these challenges is the issue of attribution of fault when AI systems cause harm—whether physical, economic, or reputational. Under prevailing corporate law principles, liability historically rests with identifiable human actors or legal entities; yet, AI complicates this paradigm by acting in ways that may not be fully anticipated or controlled by human supervisors (S. R. Kulkarni, 2024).One major legal challenge is the **"black box"** nature of many AI systems, particularly deep learning models whose internal logic is not readily interpretable. This opacity raises both procedural and substantive legal questions. Procedurally, courts and regulatory bodies face difficulty in obtaining explanations necessary to adjudicate disputes fairly; substantively, defendants can argue that harmful outcomes were unforeseeable, thus challenging negligence and strict liability claims (A. Tariq, 2025). In the corporate context, companies must demonstrate adequate oversight and risk mitigation strategies, but when an AI systems decision rationale cannot be articulated, establishing a breach of duty becomes contentious. The lack of explainability undermines not just liability determinations but also compliance with data protection and consumer protection standards that require transparency in automated decision-making (L. Fernandes and M. Singh, 2023).

Another pressing concern is the allocation of liability among stakeholders. AI solutions are often developed, deployed, and maintained through complex vendor ecosystems involving

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

developers, integrators, and end-users. Traditional contractual arrangements may attempt to allocate risk through indemnity clauses, warranties, and limitation of liability provisions. However, when AI misbehavior leads to third-party harm, contractual protections may not shield corporations from statutory liability under tort or regulatory regimes. The question of whether a developer, owner, or operator should bear liability is further blurred when AI systems evolve via machine learning, raising issues of proximate causation and foreseeability (P. R. Das and T. K. Mehta, 2024). Consequently, there is an emerging legal discourse on imposing enterprise liability models, where organizations deploying AI might be held strictly liable for harms regardless of fault, akin to strict liability in product defect cases.The introduction of regulatory frameworks specific to AI also complicates liability landscapes. Jurisdictions across the world are actively drafting AI governance laws that impose compliance obligations related to risk assessment, human oversight, and incident reporting. For example, regulatory proposals often require organizations to conduct impact assessments for high-risk AI applications and maintain documentation demonstrating safety assurances. Non-compliance with such obligations can trigger administrative penalties and civil liability, even absent traditional negligence (R. Banerjee, 2025). These evolving norms create a dual track of legal exposure: one rooted in general common law duties and another in emerging statutory duties tailored to AI risks.

A further legal challenge lies in cross-border enforcement and jurisdictional fragmentation. AI systems deployed globally interact with diverse legal regimes that vary in definitions of harm, standards of care, and thresholds of liability. Corporations must navigate this mosaic of legal expectations, which can lead to forum shopping, inconsistent judgments, and regulatory arbitrage. The absence of harmonized international legal standards for AI liability undermines predictability, increasing compliance costs for multinational enterprises while leaving victims of harm with uncertain remedies (N. Gupta, 2024).

IV. DATA PROTECTION AND PRIVACY REGULATIONS FOR CORPORATIONS

The gathering, processing, and transfer of personal data are essential to corporate operations in the digital age.. The rise of big data analytics, cloud computing, and cross-border digital services has necessitated robust data protection frameworks to safeguard individual privacy rights and ensure corporate accountability. Data protection regulations such as the European Unions General Data Protection Regulation (GDPR) set stringent standards for lawful processing, data minimisation, and transparency, influencing legislative reforms worldwide (Singh, 2021). Corporations must implement privacy by design principles and conduct regular impact

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

assessments to identify and mitigate risks associated with personal data processing, as emphasised by regulatory guidance on accountability and governance mechanisms (Banerjee and Gupta, 2022).Moreover, the extraterritorial reach of modern data protection laws imposes complex compliance obligations on multinational enterprises. For instance, non-EU firms offering goods or services to EU residents are subject to the GDPRs provisions, requiring them to appoint representatives within the EU and adhere to data subject rights such as access and erasure (Zhao, 2023). Similarly, emerging privacy statutes in Asia and Africa reflect a convergence toward baseline principles of consent, purpose limitation, and data security, compelling corporations to harmonise internal policies with diverse legal regimes (Takahashi, 2024). Failure to comply can result in significant penalties; under the GDPR, organisations may face fines up to 4% of global annual turnover, underscoring the financial and reputational risks of inadequate data governance.

At the core of corporate compliance is the integration of technological and organisational measures. Encryption, access controls, and regular audits form critical components of a privacy compliance program, complemented by employee training and incident response planning (Verma, 2022). Furthermore, the ethical dimensions of data use are receiving greater attention, with stakeholders advocating for privacy-enhancing technologies that go beyond regulatory minima to build trust with consumers and regulators alike (Alvi *et al*., 2023). As digital ecosystems evolve, corporate legal teams must remain agile, continually updating compliance frameworks to reflect legislative developments and emerging best practices in data protection.

V. CORPORATE COMPLIANCE UNDER EMERGING DATA LAWS

Corporate compliance in the digital age now includes strict duties under new data protection regulations in addition to existing regulatory frameworks. Corporations today are mandated to not only secure personal data but also demonstrate accountability in how data is collected, processed, and stored (Singh, 2024). The enforcement of comprehensive data protection regulations such as the European Unions General Data Protection Regulation (GDPR) and various national privacy laws has compelled firms to integrate compliance mechanisms into their governance structures, thereby transforming corporate legal risk strategies (Das and Roy, 2023). These evolving data laws emphasize principles such as data minimization, purpose limitation, and user consent, imposing significant operational changes on business processes and information systems (Banerjee, 2024). Furthermore, non-compliance with data protection statutes leads to heavy penalties, reputational damage, and increased scrutiny from regulators, forcing companies to adopt proactive compliance frameworks that incorporate regular audits,

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

risk assessments, and staff training (Mehta, 2023). In addition, the intersection of data protection with other regulatory domains such as cybersecurity and consumer protection law adds layers of complexity, requiring cross-functional compliance teams and continuous legal monitoring (Gupta, 2024). As data flows become increasingly global and digital services proliferate, corporate compliance functions must evolve from reactive legal checklists to strategic enablers of trust and sustainability, aligning corporate policies with both legal obligations and ethical norms (Singh and Arora, 2023). Thus, emerging data laws not only shape the legal landscape for corporations but also redefine how compliance is embedded into the corporate ethos and operational DNA.

VI. FINTECH INNOVATIONS AND THE EVOLVING LEGAL LANDSCAPE

FinTech, the integration of financial services with innovative technology, has redefined both market practices and regulatory frameworks across jurisdictions. Traditionally, financial regulation focused on protecting consumers and maintaining market stability within clearly delineated institutional boundaries. However, rapid advancements such as blockchain, peer-to-peer lending platforms, and automated financial advisors have outpaced existing legal structures, prompting regulators and scholars to rethink the legal underpinnings of financial oversight (Patel *et al*. 2024). FinTechs disruptive potential challenges conventional regulatory paradigms, demanding a balance between fostering innovation and ensuring systemic integrity.

One of the most profound ways FinTech has influenced the legal landscape is through its reliance on distributed ledger technologies (DLT), such as blockchain. These technologies enable decentralization of transactional records, reducing the need for traditional intermediaries like banks. However, decentralization raises questions about liability, jurisdiction, and enforceability of contracts executed via smart contracts. Legal scholars argue that without explicit legal recognition of smart contracts, enforceability remains ambiguous, particularly in cross-border transactions where conflicting legal systems may apply (Reddy and Singh 2023). Regulators in advanced economies are now exploring frameworks to integrate DLT within existing financial law while ensuring consumer protection. Moreover, FinTechs reliance on big data analytics and AI-driven credit scoring introduces novel legal issues related to fairness, transparency, and discrimination. Traditional credit assessments rely on standardized financial information; in contrast, AI models may use unconventional datasets, which could inadvertently encode bias against protected classes. Several legal commentators contend that the application of AI in credit decisions must be accompanied by robust transparency requirements and anti-discrimination safeguards to align with constitutional and statutory protections (Mehta

2025). The evolving jurisprudence on algorithmic accountability highlights a growing consensus that legal frameworks must adapt to address opaque decision-making processes inherent in many FinTech applications.

A central component of the FinTech legal landscape is regulatory sandboxes, which allow innovators to test financial products under regulatory supervision. Regulatory sandboxes have been adopted in Singapore, the UK, and parts of the European Union as a means to simultaneously encourage innovation and maintain oversight (Chatterjee and Rao 2024). While sandboxes offer flexibility, critics argue they may create regulatory arbitrage opportunities where companies gravitate toward lenient jurisdictions thereby undermining harmonized legal standards. This has spurred debate on the need for international cooperation in FinTech regulation, especially in areas such as cross-border payments and anti–money laundering controls. The risk management implications of FinTech are also critical to its legal assessment. For instance, digital wallets, cryptocurrency exchanges, and algorithmic trading platforms can amplify systemic risks if not adequately governed. Regulatory authorities are increasingly issuing guidelines requiring FinTech firms to adopt risk mitigation strategies comparable to those in traditional banking, such as capital adequacy requirements and cybersecurity protocols (Verma *et al*. 2023). These legal requirements seek to integrate FinTech into the broader financial safety net without stifling innovation.

VII. REGULATORY RISKS AND GOVERNANCE IN FINTECH OPERATIONS

Regulatory risks and governance in FinTech operations have become central concerns for policymakers, corporations, and legal scholars in the digital economy. FinTech enterprises operate at the intersection of traditional financial services and cutting-edge technologies, which exposes them to multifaceted regulatory risks, including compliance lapses, cyber vulnerabilities, and fragmented jurisdictional oversight (Alvi *et al*. 2023). The rapid adoption of digital payment platforms, blockchain-enabled services, and algorithmic credit assessments has outpaced the development of cohesive legal frameworks, necessitating adaptive governance mechanisms to safeguard market integrity and consumer protection (Rao and Singh 2024). A critical risk arises from regulatory arbitrage, where FinTech firms exploit gaps between overlapping supervisory regimes, leading to uncertainty in enforcement and potential systemic risk (Sharma 2022). Furthermore, the governance of data privacy within FinTech poses significant challenges; inadequate data protection can lead to breaches that not only harm customers but also invite stringent penalties under emerging data protection laws in multiple jurisdictions (Kumar and Patel 2023). Effective regulatory governance demands robust risk

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

assessment protocols, transparent reporting standards, and collaboration between regulatory bodies and industry stakeholders to balance innovation with financial stability (Chen *et al*. 2024). Another dimension of regulatory risk involves cross-border services, where inconsistent regulatory expectations impede scalability and compliance, underscoring the need for harmonized international FinTech governance frameworks (Desai 2023). In light of these complexities, scholars argue for dynamic regulatory sandboxes and continuous legal refinement to ensure that governance structures remain responsive to technological change and financial inclusion objectives (Alvi *et al*. 2023; Chen *et al*. 2024). Consequently, corporate governance in FinTech must integrate regulatory foresight, ethical standards, and risk mitigation strategies to foster trust and resilience in a rapidly evolving digital financial landscape.

VIII. CONCLUSION AND FUTURE PERSPECTIVES IN DIGITAL CORPORATE LAW

In the rapidly evolving landscape of corporate law, the integration of digital technologies such as artificial intelligence (AI), big data analytics, and FinTech solutions has introduced both significant opportunities and complex legal challenges. As corporations increasingly rely on automated decision-making and algorithmic governance, traditional legal frameworks struggle to keep pace with issues of accountability, transparency, and regulatory oversight (Sharma *et al*. 2024). The convergence of digital tools with corporate processes necessitates a proactive re-evaluation of existing statutes to ensure that legal principles of fairness, duty of care, and fiduciary responsibility remain meaningful in digital contexts.One of the most pressing legal concerns in this domain is the governance of AI systems within corporate structures. Ethical and legal questions arise when autonomous systems influence strategic decisions, risk assessments, or compliance procedures without sufficient human oversight (Alvi 2023). Corporate law must adapt to define the extent of liability when AI-driven actions cause harm or contravene regulatory mandates. Furthermore, data protection has emerged as a cornerstone of digital corporate operations. With stringent data privacy regimes such as the GDPR and evolving global standards, companies face heightened obligations to secure personal data and mitigate breaches (Khan and Mehta 2025). This trend underscores the imperative for robust internal compliance mechanisms that align with jurisdictional expectations.

FinTech innovations, while enabling faster and more inclusive financial services, present unique regulatory challenges. The decentralized nature of blockchain-based systems and digital assets tests the limits of existing financial and corporate legal frameworks (Verma 2024). Regulatory bodies worldwide are experimenting with sandbox approaches and adaptive oversight models to balance innovation with market stability. Nonetheless, persistent gaps

remain in areas such as cross-border digital transactions, consumer protection, and anti-money laundering enforcement. Addressing these gaps will require sustained dialogue among regulators, industry stakeholders, and legal scholars to formulate harmonized standards that can be effectively enforced.Looking forward, future research and policy formulation must emphasize interdisciplinary collaboration. Legal scholars should engage with technologists to understand the technical nuances that influence legal interpretations and enforcement strategies (Rao and Gupta 2024). Additionally, corporate leaders must cultivate a culture of legal foresight, embedding digital ethics into governance models to preempt legal conflicts and bolster stakeholder trust. Regulatory agility, supplemented by periodic reviews of digital corporate practices, will be critical to managing the dynamic interplay between innovation and legal compliance. Overall, the future of digital corporate law lies in its capacity to uphold fundamental legal values while embracing technological transformation.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

IX. REFERENCES

- A. Tariq, "Opaque Algorithms and Legal Liability: Challenges in Interpreting AI Decisions," *Int. Review of Tech Law* 12(1): 89–105 (2025).
- Chatterjee, S., *and* Rao, K. (2024). Regulatory Sandboxes and Innovation Governance in FinTech. Journal of Financial Regulation Insights, 45–59.
- Desai, P. (2025). Consumer Protection Challenges in FinTech Markets. International Review of Financial Law, 78–92.
- K. Mehta, Corporate Risk Management in the Digital Age: Ensuring Compliance with Emerging Data Laws, in International Journal of Corporate Governance 29–45 (2023).
- K. R. Singh, Corporate Data Governance: Legal Frameworks and Challenges, in Advances in Digital Law and Policy 55–68 (2024).
- L. Chen, M. Gupta *and* R. Banerjee, *Governance Mechanisms in Emerging Financial Technologies*, *Corporate Governance Review* 33–54 (2024).
- L. Fernandes *and* M. Singh, "Transparency and Consumer Protection in Automated Decision-Making," *Corporate Law Journal* 15(4): 322–39 (2023).
- L. Singh, *Regulatory Agility in Corporate Law for Digital Innovations*, *Global Legal Perspectives on Technology* 8(1): 12–29 (2025)
- L. T. Das *and* M. Roy, Data Protection Compliance: Corporate Obligations and Ethical Impacts, in Corporate Law Review 102–17 (2023).
- M. Rao *and* K. Gupta, *Interdisciplinary Approaches to Digital Law and Policy*, *Law and Technology Quarterly* 4(4): 77–95 (2024).
- Mehta, A. (2025). AI, Credit Scoring, and Legal Accountability. Computational Finance and Law Journal, 12–29.
- Mustafa Kenan Ustahaliloğlu, *Artificial intelligence in corporate governance*, 7(1) Corporate Law *and* Governance Rev. 123–134 (2025). Göktürk Kalkan, *The Impact of Artificial Intelligence on Corporate Governance*, J. of Corporate Finance Research (2024).
- N. Balaji Ganesh *et al*., *Corporate Governance in the Age of AI: Ethical Oversight and Accountability Frameworks*, J. of Information Systems Eng'g *and* Mgmt. (2025).
- N. Gupta, "Jurisdictional Challenges in Global AI Liability Frameworks," *Global Legal Studies* 11(3): 201–28 (2024).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

- P. R. Das *and* T. K. Mehta, "Liability Allocation in Multi-Stakeholder AI Ecosystems," *Law and Emerging Tech.* 9(3): 150–74 (2024).
- P. Sharma, *Navigating FinTech Risks: An Integrative Legal Perspective*, *Journal of Corporate Law and Technology* 78–92 (2022).
- P. Singh *and* N. S. Arora, Ethical Dimensions of Data Compliance in Corporations, in Ethics *and* Corporate Responsibility Journal 89–104 (2023).
- Patel, R., Gupta, S., *and* Khan, T. (2024). Disruptive Technologies in Financial Services: Legal Implications. Global Financial Technology Review, 102–118.
- R. Banerjee, "Regulatory Obligations and Civil Liability in AI Governance," *Regulatory Studies Q.* 7(1): 77–98 (2025).
- R. Rao *and* T. Singh, *Regulatory Frameworks for Digital Financial Services: Balancing Innovation and Compliance*, in *Advances in Financial Law and Technology* 45–68 (2024).
- R. V. Gupta, Integrating Cybersecurity and Data Protection Compliance: Legal Challenges for Modern Corporations, in Technology Law Insights 117–30 (2024).
- R. Verma, *FinTech Regulation and Legal Challenges in Emerging Markets*, *Digital Finance Studies* 6(2): 88–109 (2024).
- Reddy, L., *and* Singh, N. (2023). Smart Contracts and Legal Enforceability in Cross-Border FinTech. Journal of Emerging Legal Technologies, 33–48.
- S. Banerjee, Privacy by Design in Corporate Systems: Legal and Managerial Perspectives, in Journal of Data Law and Ethics 73–86 (2024).
- S. Khan *and* A. Mehta, *Data Protection Compliance in Global Corporations*, *International Corporate Law Journal* 9(3): 101–120 (2025).
- S. Kumar *and* A. Patel, *Data Protection Challenges in FinTech Enterprises: Legal Responses and Governance Models*, in *Data Rights and Regulation* 101–19 (2023).
- S. R. Kulkarni, "Attribution of Fault in Autonomous Systems: A Corporate Law Perspective," *J. of AI and Law* 8(2): 45–62 (2024).
- Sharma, P. Singh *and* R. Das, *AI Governance and Corporate Accountability in the Digital Era*, *Journal of Tech Law Review* 12(1): 45–67 (2024).
- V. Desai, *Cross-Border FinTech Regulation: Harmonization and Legal Complexities*, in *International Financial Law Journal* 59–77 (2023).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

- Verma, D., Shah, M., *and* Iyer, L. (2023). Risk Governance in Digital Finance Platforms. Financial Law and Risk Journal, 201–216.
- Vineeta *and* Dr. Sonia Pajoria, *Impact of Artificial Intelligence on Corporate Governance*, 8(2) Int'l J. of Law Management *and* Humanities 4319–4336 (2025).
- Z. M. Alvi, *The Impact of Surveillance on Human Rights: Exploring the Ethical and Legal Implications of Mass Surveillance Programs*, in *Bridging the Gaps: Research Insights* 214–22 (2023).

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]