

Corporate Governance and Legal Accountability in the Age of Digital Transformation

Dodi Rusmana¹ , Mohamad Ali Syaifudin² , Yudha Ginanjar³ , Anwar Sadat⁴ , Ethan Tan⁵

¹Universitas Islam Jakarta, Indonesia

²Sekolah Tinggi Ilmu Hukum dan Politik Pelopor Bangsa, Indonesia

³Sekolah Tinggi Ilmu Hukum dan Politik Pelopor Bangsa, Indonesia

⁴Universitas Islam Jakarta, Indonesia

⁵National University of Singapore (NUS), Singapore

ABSTRACT

Background. Digital transformation has fundamentally reshaped corporate decision-making by integrating artificial intelligence, automated systems, data analytics, and external digital infrastructures, creating new challenges for governance oversight and legal accountability.

Purpose. This study aimed to examine how digitally distributed decision-making influences accountability gaps and to identify governance mechanisms that preserve responsibility within complex human–technology systems.

Method. A comparative socio-legal mixed-methods design combined corporate governance surveys, legal and regulatory analysis, organizational document review, semi-structured interviews, and cross-case analysis.

Results. The findings showed that greater digital integration increased accountability ambiguity when formal authority, operational control, technical knowledge, and intervention capacity were poorly aligned. Board digital competence, human oversight, algorithmic transparency, auditability, internal controls, and regulatory preparedness significantly strengthened accountability clarity and reduced risks associated with distributed decision-making.

Conclusion. The study concludes that digital transformation does not inherently weaken legal accountability; accountability deteriorates when governance structures fail to evolve alongside technological influence.

KEYWORDS

Algorithmic Accountability, Corporate Governance, Digital Transformation

INTRODUCTION

Digital transformation has fundamentally altered the organizational, technological, and regulatory environments in which contemporary corporations operate. Artificial intelligence, algorithmic decision-making, big-data analytics, cloud computing, automated systems, digital platforms, and interconnected information infrastructures increasingly influence strategic planning, operational processes, customer relationships, risk assessment, and managerial decision-making. These developments offer

Citation: Rusmana, D., Syaifudin, A M., Ginanjar, Y., Sadat, A & Tan, E. (2026). Corporate Governance and Legal Accountability in the Age of Digital Transformation. *Rechtsnormen Journal of Law*, 4(4), 267–285.

<https://doi.org/10.70177/rjl.v4i4.4229>

Correspondence:

Dodi Rusmana,
drupiah506@gmail.com

Received: February 12, 2026

Accepted: May 15, 2026

Published: August 13, 2026



substantial opportunities for efficiency, innovation, competitiveness, and organizational adaptability. Their integration also changes how corporate decisions are produced, documented, delegated, and monitored, creating governance challenges that extend beyond conventional models of managerial oversight. Corporate governance must consequently address not only relationships among shareholders, boards, executives, and stakeholders but also the growing influence of complex digital systems on organizational authority and decision-making (Cowin, 2025; Gkasis, 2026).

Corporate governance has traditionally been structured around principles of accountability, transparency, responsibility, fairness, oversight, and the protection of stakeholder interests. Digital transformation complicates the practical application of these principles because organizational decisions may increasingly depend on automated systems, third-party technology providers, opaque algorithms, and large-scale data processing. A decision that causes financial, social, discriminatory, privacy-related, or reputational harm may involve multiple actors across interconnected technological and organizational processes. Determining who exercised meaningful control, who should have anticipated the risk, and who bears responsibility for the resulting consequences therefore becomes increasingly difficult (Aliaga, 2026; Balan, 2025).

Legal accountability acquires particular significance within this changing environment. Corporate law, data-protection regulation, cybersecurity obligations, consumer protection, competition law, employment law, and emerging artificial-intelligence governance frameworks increasingly intersect in digitally transformed organizations. Boards and senior executives are expected to exercise appropriate oversight even when the technical complexity of digital systems exceeds traditional managerial expertise. Digital transformation therefore raises a fundamental governance question: how can legal accountability remain identifiable, enforceable, and institutionally meaningful when corporate decision-making becomes increasingly distributed among human actors, automated systems, data infrastructures, and external technology providers?

The central problem concerns the growing accountability gap between corporate decision-making authority and the technological systems through which decisions are increasingly executed. Traditional governance frameworks generally assume that identifiable human actors exercise authority and can be held responsible for organizational decisions. Algorithmic systems complicate this assumption because decision processes may involve automated recommendations, machine-learning outputs, dynamic data models, and technically opaque procedures. Corporate actors may rely heavily on automated outputs without fully understanding how particular conclusions were generated, creating uncertainty regarding responsibility when those outputs produce harmful, unlawful, biased, or discriminatory consequences (Cicu, 2024; Yazici, 2026).

A second problem arises from the fragmentation of responsibility across corporate governance structures and digital supply chains. Boards may approve digital-transformation strategies, executives may oversee implementation, technology departments may manage systems, employees may use automated tools, and external vendors may design algorithms or provide cloud-based infrastructure. Such distributed arrangements can create accountability diffusion, in which each actor controls only part of the decision process. Contractual outsourcing does not necessarily eliminate corporate legal obligations, yet unclear governance structures may allow organizations to treat technological failures as technical problems rather than failures of oversight, due diligence, compliance, or fiduciary responsibility (Bressane, 2026; Kunz, 2026).

A third problem concerns the uneven development of legal and governance frameworks relative to technological change. Corporate digitalization often advances faster than organizational policies, board competencies, audit mechanisms, and regulatory standards. Existing governance

principles remain relevant, but their application to algorithmic transparency, cybersecurity, data governance, automated decision-making, and artificial-intelligence risk is not always clearly operationalized. Regulatory fragmentation across jurisdictions further complicates compliance for multinational corporations, producing uncertainty about applicable standards of accountability and the appropriate allocation of legal responsibility (KRAFZIK, 2026; Singh, 2025).

This study aims to examine how digital transformation reshapes corporate governance structures and the allocation of legal accountability within contemporary organizations. The research focuses on the relationship between technological adoption, board oversight, managerial responsibility, organizational control, and legal obligations. Particular attention is directed toward determining how corporations can maintain identifiable lines of accountability when decision-making processes increasingly incorporate artificial intelligence, automated systems, data analytics, and third-party digital infrastructure.

The study seeks to analyze whether established corporate governance principles remain sufficient for addressing risks generated by digitally mediated decision-making. Accountability, transparency, fiduciary responsibility, due diligence, risk management, internal control, and stakeholder protection are examined in relation to emerging challenges involving algorithmic opacity, cybersecurity, data misuse, automated discrimination, privacy violations, and technological dependency. The analysis aims to identify circumstances in which conventional governance mechanisms remain effective and areas where additional digital-governance mechanisms are required (Ababneh, 2025; Manoharan, 2026).

The research further aims to develop an integrated analytical framework connecting Digital Transformation - Governance Complexity → Accountability Risks - Governance and Legal Safeguards - Responsible Corporate Outcomes. Board digital competence, algorithmic transparency, human oversight, auditability, internal controls, risk governance, and regulatory clarity are examined as mechanisms capable of reducing accountability gaps. This framework is intended to explain not merely whether digital transformation creates legal risks, but how organizational governance can allocate, trace, and enforce responsibility across increasingly complex human–technology decision systems (Khalil, 2026; Schuessler, 2026).

Existing scholarship on corporate governance has extensively examined board composition, ownership structures, executive accountability, shareholder protection, agency problems, corporate transparency, and financial performance. Digital transformation research, by contrast, has often emphasized technological adoption, innovation capability, operational efficiency, organizational agility, and competitive advantage. These bodies of literature frequently develop in parallel, leaving insufficient theoretical integration between digital transformation and the fundamental governance question of who exercises authority and bears responsibility when technology becomes embedded in corporate decision-making.

Research on artificial intelligence ethics and digital regulation has generated important discussions concerning algorithmic bias, explainability, privacy, cybersecurity, transparency, and responsible AI. A substantial portion of this literature focuses on ethical principles or technical safeguards without fully connecting these concerns to corporate governance structures such as board duties, fiduciary obligations, internal controls, compliance systems, audit functions, and executive responsibility. Ethical AI principles alone may not ensure accountability unless they are translated into enforceable organizational duties and identifiable decision rights (Mamilla, 2025; Naz, 2026).

Comparative legal scholarship also reveals a gap between regulatory development and integrated corporate accountability analysis. Different jurisdictions increasingly regulate data

protection, cybersecurity, digital platforms, and artificial intelligence through distinct legal instruments, yet corporations often operate across multiple regulatory environments simultaneously. Limited research systematically examines how regulatory fragmentation interacts with internal governance structures to create or reduce accountability gaps. Greater conceptual integration is therefore needed between corporate governance theory, digital governance, organizational accountability, and legal-regulatory analysis (Alyami, 2026; Ismail, 2025).

The principal novelty of this study lies in conceptualizing digital transformation as a transformation of corporate accountability architecture rather than merely a process of technological modernization. The proposed framework distinguishes between formal authority, technological agency, and legal accountability, recognizing that these dimensions may become misaligned in digitally mediated organizations. A corporation may formally assign decision authority to managers while operational decisions are substantially shaped by algorithmic systems. The study therefore introduces the concept of an algorithmic accountability gap to describe situations in which technological influence expands while human responsibility, oversight, and traceability become increasingly ambiguous (Sharma, 2025; Toukabri, 2025).

A second element of novelty lies in integrating corporate governance and legal accountability through a proposed Digital Corporate Accountability Framework. The framework connects Digital Transformation - Distributed Decision-Making - Accountability Gap - Governance Safeguards - Legal Accountability, with board digital competence, algorithmic transparency, human oversight, auditability, internal control, and regulatory clarity functioning as accountability-enabling mechanisms. This perspective rejects the misleading assumption that technology itself can bear legal responsibility in the same institutional sense as corporate actors. Automated systems may exercise functional influence, but corporations and legally recognized actors remain responsible for designing, deploying, supervising, auditing, and governing those systems within applicable legal frameworks.

The study is justified by the increasing urgency of establishing governance arrangements capable of supporting innovation without allowing technological complexity to become a shield against accountability. Effective digital governance should not require boards to understand every technical detail of artificial intelligence or algorithmic architecture, but it should require sufficient competence to ask critical questions, establish risk boundaries, demand reliable assurance, identify responsible decision-makers, and intervene when digital systems create unacceptable risks. The broader contribution of this research lies in reframing the central governance question from “Who made the decision?” toward “Who had authority, who exercised meaningful control, who could reasonably foresee the risk, who had the capacity to intervene, and who should legally answer for the consequences?” This reframing provides a more robust foundation for corporate accountability in an era when human judgment and technological systems are increasingly intertwined (Ahdadou, 2026; Canato, 2026).

RESEARCH METHODOLOGY

This study employed a comparative socio-legal mixed-methods design to examine how digital transformation reshapes corporate governance structures and the allocation of legal accountability within increasingly technology-dependent organizations. The research integrated quantitative organizational evidence with qualitative legal and governance analysis to investigate the relationship between digital transformation, distributed decision-making, accountability risks, and governance safeguards. The analytical framework followed the pathway Digital Transformation - Distributed Decision-Making - Accountability Gap - Governance Safeguards - Legal

Accountability, allowing the study to examine not only whether digitalization creates new governance risks but also the organizational and legal mechanisms through which those risks can be identified, controlled, and attributed (Ishkhanyan, 2026; Yigitcanlar, 2026).

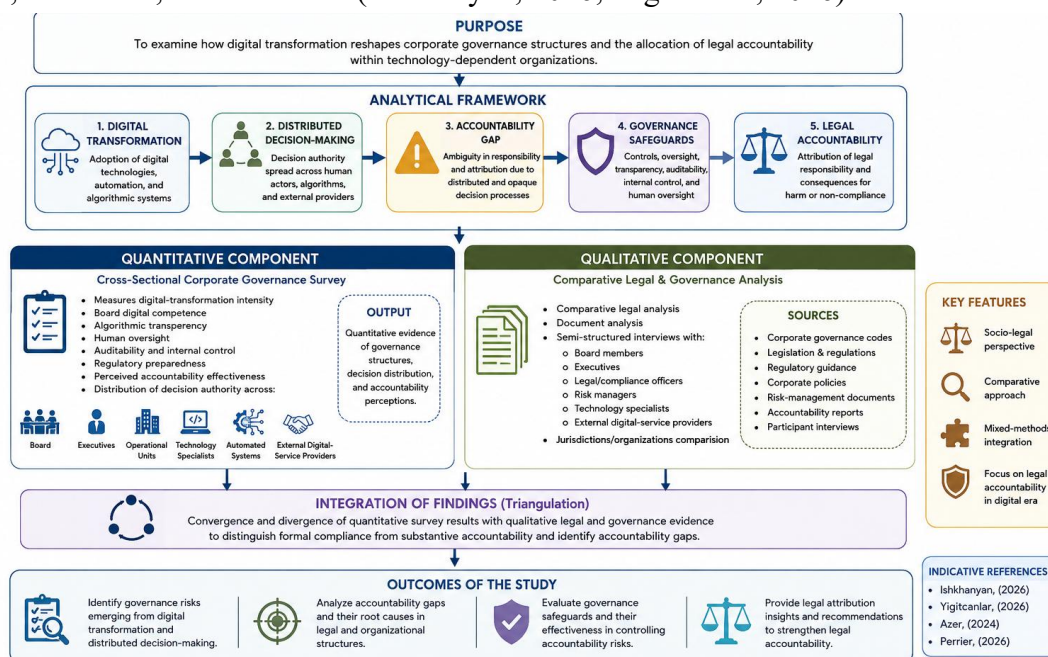


Figure 1. Research Design of the Comparative Socio-Legal Mixed-Methods Study on Digital Transformation, Distributed Decision-Making, and Legal Accountability

The quantitative component used a cross-sectional corporate governance survey to assess digital-transformation intensity, board digital competence, algorithmic transparency, human oversight, auditability, internal control, regulatory preparedness, and perceived accountability effectiveness. The survey was designed to capture how organizations distribute decision authority across boards, executives, operational units, technology specialists, automated systems, and external digital-service providers. Particular attention was given to situations in which formal decision authority remained with human actors while operational influence was increasingly exercised through algorithmic recommendations or automated processes.

The qualitative component employed comparative legal analysis, document analysis, and semi-structured interviews to examine how formal legal obligations corresponded with actual corporate governance practices. Relevant corporate governance codes, legislation, regulatory guidance, corporate policies, risk-management documents, and publicly available accountability reports were analyzed alongside participant accounts. The integration of these sources enabled the study to distinguish formal compliance from substantive accountability and to identify areas in which governance structures appeared adequate on paper but remained ambiguous in practice (Azer, 2024; Perrier, 2026).

The target population consisted of corporations undergoing substantial digital transformation and organizational actors directly involved in corporate governance, digital strategy, risk management, legal compliance, internal audit, information technology, data governance, and artificial-intelligence oversight. Eligible organizations were required to demonstrate meaningful adoption of digital technologies such as artificial intelligence, automated decision systems, advanced analytics, cloud infrastructure, algorithmic platforms, or data-intensive operational systems (Bohlens, 2025; Nosikov, 2026).

A purposive stratified sampling strategy was used to capture variation across industries with different levels of digital intensity and regulatory exposure. Participating organizations were selected from sectors such as financial services, telecommunications, technology, manufacturing, retail, healthcare-related industries, and digitally mediated services where appropriate. Organizational size, ownership structure, technological maturity, and regulatory environment were considered during sampling to avoid treating digitally transformed corporations as a homogeneous category.

Survey respondents included board members, senior executives, corporate legal officers, compliance professionals, internal auditors, risk managers, information-technology leaders, data-governance personnel, and managers responsible for digital-transformation initiatives. Respondents were required to possess sufficient knowledge of organizational decision-making, digital systems, governance controls, or legal-accountability arrangements. This criterion was necessary because general employee perceptions would not provide adequate evidence concerning board oversight, accountability allocation, or corporate legal responsibilities.

A purposive subsample was selected for semi-structured interviews based on professional role, organizational characteristics, and involvement in digitally mediated decision-making. Participants representing legal, governance, technological, and managerial perspectives were included to capture potential differences in how accountability was understood across organizational functions. Sampling continued until sufficient conceptual depth and thematic saturation were achieved for the principal categories under investigation (Bose, 2026; Taşkale, 2026).

The comparative legal component examined selected jurisdictions representing different approaches to corporate governance, data protection, cybersecurity, automated decision-making, and artificial-intelligence regulation. Jurisdictions were selected according to their regulatory relevance, availability of comparable legal materials, and significance to corporate digital governance. The comparative approach was intended to identify convergent principles and meaningful regulatory differences rather than rank legal systems according to a single standard.

The primary quantitative instrument was the Digital Corporate Governance and Accountability Questionnaire, developed from established corporate-governance principles and contemporary literature on digital governance, responsible artificial intelligence, risk management, and organizational accountability. The instrument measured several dimensions, including digital-transformation intensity, distributed decision-making, board digital competence, algorithmic transparency, human oversight, auditability, internal control effectiveness, regulatory preparedness, and perceived legal-accountability clarity.

Digital-transformation intensity was measured through indicators of organizational dependence on automated systems, artificial intelligence, advanced analytics, cloud-based infrastructure, and data-driven decision processes. Distributed decision-making was assessed by examining the extent to which significant corporate decisions involved interactions among human managers, algorithmic recommendations, automated processes, technology teams, and external providers. Accountability-gap indicators measured ambiguity regarding who held authority, exercised meaningful control, possessed relevant knowledge, had the capacity to intervene, and ultimately bore responsibility for digitally mediated decisions.

Governance safeguards were assessed through measures of board-level digital oversight, documented decision rights, human-in-the-loop procedures, algorithmic transparency, audit mechanisms, risk-assessment protocols, escalation procedures, vendor governance, cybersecurity controls, and accountability documentation. Legal-accountability measures examined perceived

clarity of duties, traceability of decisions, regulatory compliance, responsibility allocation, and organizational capacity to identify accountable actors following digital failures or harmful outcomes (Hinov, 2026; Okuno, 2025).

A structured legal and document-analysis matrix was used to examine legislation, regulatory guidance, governance codes, corporate policies, risk frameworks, audit documents, and accountability reports. The matrix coded provisions relating to fiduciary duties, due diligence, oversight obligations, data protection, cybersecurity, automated decision-making, transparency, auditability, human intervention, third-party responsibility, and enforcement mechanisms. This structure enabled systematic comparison between formal regulatory expectations and organizational governance practices (Hinov, 2026; Okuno, 2025).

Instrument quality was established through expert review involving specialists in corporate governance, business law, digital regulation, organizational risk, and research methodology. Content validity was assessed to determine whether the instruments adequately represented the conceptual dimensions of digital corporate accountability. Pilot testing was conducted with participants possessing relevant professional backgrounds, and reliability and construct validity were examined before the full quantitative analysis.

The research began with ethical approval, organizational recruitment, participant information procedures, and informed consent. Participating corporations and professionals were informed about the study's objectives, confidentiality arrangements, data-management procedures, and voluntary nature of participation. Organizational identities were anonymized where required to reduce reputational risk and encourage participants to discuss governance weaknesses and accountability ambiguities openly.

The first empirical stage involved the collection and analysis of relevant legal and regulatory materials. Corporate law provisions, governance codes, data-protection rules, cybersecurity requirements, artificial-intelligence regulations, regulatory guidance, and relevant accountability standards were systematically reviewed. The analysis identified the formal duties imposed on boards, executives, corporations, and other responsible actors when digital technologies influenced organizational decisions (Amayreh, 2026; Torralba, 2026).

The second stage involved the collection of corporate governance documents and publicly available organizational materials. Digital-governance policies, annual reports, risk-management frameworks, AI principles, cybersecurity policies, board committee structures, audit procedures, and accountability disclosures were analyzed using the document-analysis matrix. Documentary evidence was used to identify how organizations formally allocated responsibility and whether governance mechanisms addressed the distinctive risks associated with digitally mediated decision-making.

The third stage consisted of administering the corporate governance survey to eligible participants. Responses were collected through a secure research platform and screened for completeness, response quality, and eligibility. Descriptive statistics were calculated to characterize organizational digitalization, governance safeguards, and perceived accountability clarity. Reliability and factor analyses were conducted to evaluate the measurement properties of the principal constructs.

Inferential analysis examined relationships among digital transformation, distributed decision-making, accountability gaps, governance safeguards, and legal-accountability effectiveness. Multiple regression or structural equation modeling was used where sample size and statistical assumptions permitted. Mediation analysis examined whether distributed decision-making and

accountability ambiguity explained the relationship between digital-transformation intensity and accountability risks.

Moderation analysis examined whether governance safeguards reduced the negative relationship between digitally distributed decision-making and accountability clarity. Board digital competence, human oversight, algorithmic transparency, auditability, internal controls, and regulatory preparedness were evaluated as potential protective mechanisms. This analysis tested whether technological complexity necessarily weakened accountability or whether strong governance arrangements could preserve identifiable responsibility despite increasingly complex digital systems (Ahdadou, 2026; Bose, 2026).

The fourth stage involved semi-structured interviews with selected participants. Interviews were recorded with permission, transcribed, anonymized, and analyzed using thematic analysis. Coding focused on decision authority, technological influence, responsibility attribution, oversight practices, accountability diffusion, regulatory uncertainty, vendor relationships, and organizational responses to digital failures. Particular attention was given to discrepancies between formal governance arrangements and actual decision-making practices.

Cross-case analysis compared organizations with stronger and weaker accountability structures. Cases were examined according to digital maturity, board oversight, technological dependency, regulatory exposure, and the clarity of responsibility allocation. The analysis sought to identify recurring patterns in which formal authority remained identifiable but meaningful operational control became distributed across technological and organizational actors.

The legal and empirical findings were integrated through a triangulation process. Formal legal duties were compared with survey patterns, corporate documents, and interview evidence to identify convergence and divergence between regulatory expectations and organizational practice. This procedure allowed the study to determine whether apparent accountability gaps resulted from inadequate law, weak implementation, unclear internal governance, technological opacity, or combinations of these factors.

The final interpretation applied the Digital Corporate Accountability Framework: Digital Transformation - Distributed Decision-Making - Accountability Gap - Governance Safeguards - Legal Accountability. Responsibility was evaluated according to five interrelated questions: who possessed formal authority, who exercised meaningful control, who had access to relevant knowledge, who could reasonably foresee or mitigate the risk, and who had the capacity to intervene. This analytical approach avoided treating artificial intelligence or automated systems as independent bearers of legal responsibility and instead examined how corporations and legally recognized actors remained accountable for the design, deployment, supervision, auditing, and consequences of digitally mediated decision systems (Ayhan, 2025; Vartiak, 2025).

RESULT AND DISCUSSION

The analysis revealed substantial variation in how corporations governed digitally mediated decision-making and allocated responsibility across organizational structures. Survey data from 286 governance and professional respondents representing digitally transforming organizations showed a high overall level of digital-transformation intensity ($M = 4.12$, $SD = 0.58$) and distributed decision-making ($M = 3.89$, $SD = 0.64$). Governance safeguards were moderately developed ($M = 3.57$, $SD = 0.69$), while perceived legal-accountability clarity remained comparatively lower ($M = 3.31$, $SD = 0.74$). The accountability-gap score reached a moderate-to-high level ($M = 3.68$, $SD = 0.71$), indicating that increasing technological integration was frequently accompanied by

uncertainty concerning who exercised meaningful control and who should answer for digitally mediated outcomes.

Table 1. Descriptive Statistics for Digital Corporate Governance and Accountability Variables

Variable	Mean	SD	Interpretation
Digital-Transformation Intensity	4.12	0.58	High
Distributed Decision-Making	3.89	0.64	High
Accountability Gap	3.68	0.71	Moderate High
Board Digital Competence	3.42	0.73	Moderate
Algorithmic Transparency	3.18	0.77	Moderate
Human Oversight	3.71	0.68	Moderate High
Auditability	3.39	0.72	Moderate
Internal Control Effectiveness	3.74	0.65	Moderate High
Regulatory Preparedness	3.36	0.75	Moderate
Legal-Accountability Clarity	3.31	0.74	Moderate

Secondary analysis of governance policies, regulatory materials, annual reports, risk-management frameworks, and digital-governance documents revealed a similar pattern. Most organizations formally recognized cybersecurity, privacy, data protection, and operational technology risks, but fewer documents explicitly addressed responsibility for algorithmic recommendations, automated decisions, model errors, or third-party AI systems. Legal and regulatory materials generally preserved organizational and human responsibility, although operational guidance concerning how responsibility should be allocated across complex digital decision chains varied considerably.

The descriptive findings indicate that technological transformation was progressing more rapidly than the development of corresponding accountability structures. Organizations had widely integrated digital systems into strategic and operational processes, yet board competence, algorithmic transparency, auditability, and regulatory preparedness had not developed at an equivalent level. This imbalance created conditions in which digital systems could exert substantial influence over decisions without equally clear mechanisms for tracing responsibility when those decisions generated harmful or legally problematic consequences.

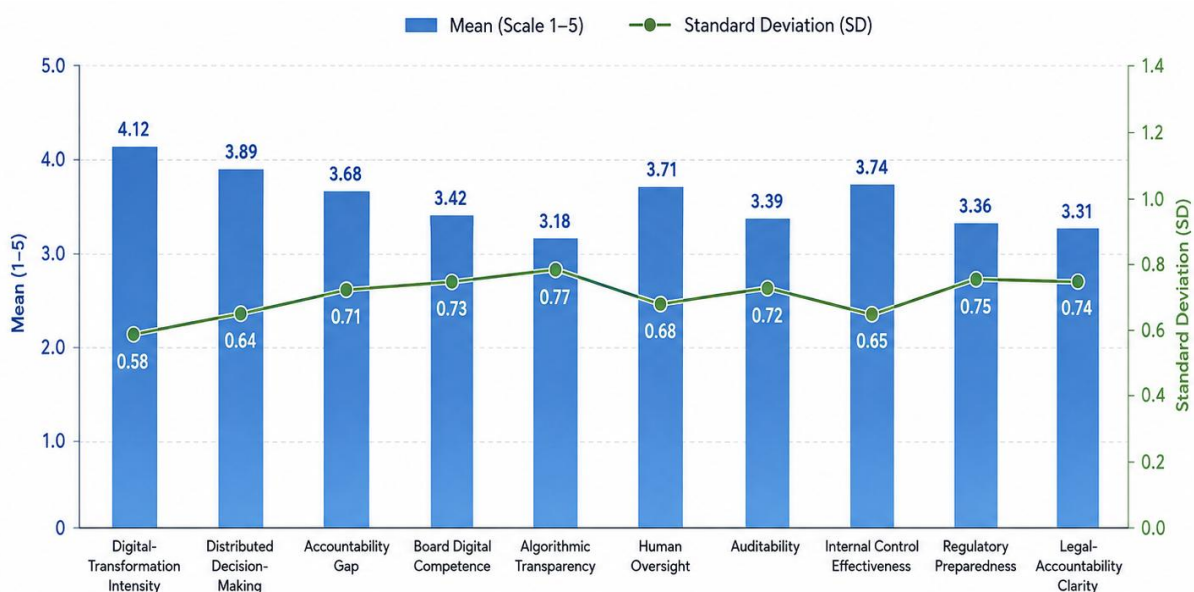


Figure 2. Descriptive Statistics of Digital Corporate Governance and Accountability Variables

The document analysis further showed that formal governance structures did not always reflect actual patterns of technological influence. Corporate policies frequently assigned ultimate responsibility to boards or senior management, while operational decisions were increasingly shaped by data models, automated recommendations, external technology vendors, and specialized technical teams. Formal authority therefore remained identifiable, but meaningful control was often distributed, creating a practical gap between who was legally responsible and who possessed sufficient knowledge or capacity to influence the underlying digital process.

Analysis of governance safeguards showed considerable differences across organizations. Human oversight and general internal controls were more established than algorithmic transparency and technical auditability. Most respondents reported that employees or managers retained some authority to review or override automated outputs, but fewer organizations maintained systematic documentation explaining when human intervention occurred, how algorithmic recommendations influenced final decisions, or who was responsible for validating the reliability of automated systems.

Interview evidence revealed recurring uncertainty concerning third-party digital providers. Participants commonly distinguished between technical responsibility for system design and corporate responsibility for decisions made using those systems. Several respondents reported that contractual arrangements allocated technical obligations to vendors, yet internal governance policies did not always specify whether vendor failures altered the corporation's responsibility toward customers, employees, regulators, or other affected stakeholders. This ambiguity was especially visible in cases involving cloud services, automated risk scoring, algorithmic recruitment, and outsourced analytics.

Multiple regression analysis indicated that distributed decision-making significantly predicted a larger accountability gap ($\beta = .48, p < .001$), even after controlling for organizational size, sector, digital maturity, and regulatory exposure. Digital-transformation intensity also showed a positive relationship with accountability ambiguity ($\beta = .29, p < .001$), although this relationship weakened when governance safeguards were introduced into the model. The findings suggest that digital transformation itself was not sufficient to produce accountability failure; the risk became greater when technological influence expanded without corresponding oversight and responsibility structures.

Governance safeguards significantly predicted greater legal-accountability clarity ($\beta = .52, p < .001$). Board digital competence ($\beta = .21, p = .003$), human oversight ($\beta = .27, p < .001$), auditability ($\beta = .24, p < .001$), and regulatory preparedness ($\beta = .19, p = .008$) each contributed positively to accountability clarity. The interaction between distributed decision-making and governance safeguards was statistically significant ($\beta = -.18, p = .011$), indicating that stronger governance arrangements reduced the negative accountability effects associated with increasingly distributed digital decision processes.

Correlation analysis revealed a strong positive relationship between distributed decision-making and the accountability gap ($r = .57, p < .001$). Algorithmic transparency was negatively associated with accountability ambiguity ($r = -.43, p < .001$), while auditability showed a positive relationship with legal-accountability clarity ($r = .51, p < .001$). Board digital competence was positively associated with both human oversight ($r = .46, p < .001$) and regulatory preparedness ($r = .49, p < .001$), suggesting that digitally competent boards were more likely to establish governance mechanisms capable of translating technological risks into identifiable oversight responsibilities.

Mediation analysis indicated that distributed decision-making partially mediated the relationship between digital-transformation intensity and accountability gaps. Organizations with

greater technological integration tended to distribute operational influence across more actors and systems, which subsequently increased ambiguity regarding responsibility. Strong governance safeguards weakened this pathway by improving decision traceability, defining intervention rights, documenting human oversight, and clarifying escalation procedures. Accountability therefore depended not simply on how extensively technology was used but on how authority and control were structured around that technology.

A financial-services organization provided a representative case of a relatively mature digital-accountability structure. The organization used algorithmic systems for risk assessment and customer-related decisions but maintained documented human-review thresholds, model-validation procedures, audit trails, escalation mechanisms, and clearly assigned executive responsibility. High-risk decisions could not be finalized solely through automated outputs, and model performance was periodically reviewed by independent risk and audit functions. Interview participants demonstrated a relatively consistent understanding of who could approve, challenge, suspend, or investigate automated decision processes.

A contrasting case involved a digitally intensive service organization that relied heavily on a third-party algorithmic platform. Managers routinely used automated recommendations, but responsibility for model validation, data quality, decision review, and adverse outcomes remained fragmented across the corporation and technology provider. Internal staff described the platform as technically controlled by the vendor, while contractual documents emphasized that final business decisions remained the corporation's responsibility. A problematic automated recommendation therefore exposed an accountability gap: legal responsibility remained organizationally identifiable, but operational knowledge and meaningful control were distributed across actors who possessed only partial visibility into the decision process.

The comparison between the two cases demonstrates that algorithmic complexity does not inevitably eliminate accountability. The financial-services organization preserved identifiable responsibility by combining technological adoption with explicit decision rights, human-review thresholds, independent validation, audit trails, and escalation procedures. Responsibility remained traceable because governance mechanisms connected formal authority with meaningful control and access to relevant information.

The contrasting case demonstrates how outsourcing can intensify accountability diffusion without transferring legal responsibility in an equivalent manner. Reliance on a third-party provider reduced direct organizational visibility into technical processes, yet the corporation continued to use algorithmic outputs in decisions affecting stakeholders. Contractual delegation of technical functions did not automatically remove governance duties related to due diligence, oversight, risk management, or legal compliance. The central vulnerability therefore arose from a mismatch between operational dependency and governance capacity.

The overall findings support the proposed pathway Digital Transformation - Distributed Decision-Making - Accountability Gap - Governance Safeguards - Legal Accountability. Greater digitalization was associated with more distributed patterns of operational influence, which increased accountability ambiguity when decision rights, oversight responsibilities, technical knowledge, and intervention authority were insufficiently aligned. Board digital competence, human oversight, algorithmic transparency, auditability, internal controls, and regulatory preparedness substantially reduced these risks.

The findings suggest that the central legal-governance challenge of digital transformation is not that artificial intelligence or algorithms replace human legal responsibility, but that they can obscure the pathways through which responsibility should be identified and enforced. Effective

digital corporate governance therefore requires accountability to be evaluated through interconnected dimensions of formal authority, meaningful control, access to relevant knowledge, reasonable foreseeability of risk, and capacity to intervene. Corporate accountability remains strongest when organizations can demonstrate not merely who formally approved a digital system, but who was responsible for understanding its risks, monitoring its operation, challenging its outputs, and responding when its consequences became legally or ethically unacceptable.

The findings demonstrate that digital transformation is reshaping corporate governance not merely by introducing new technologies but by redistributing influence over organizational decision-making. Corporations with higher levels of digital integration increasingly relied on artificial intelligence, automated systems, advanced analytics, cloud infrastructure, and external technology providers to support or execute important decisions. Formal authority generally remained assigned to boards, executives, and managers, while meaningful operational influence became distributed across human actors, technological systems, and external providers. This divergence created accountability gaps when governance structures failed to evolve at the same pace as technological adoption.

Distributed decision-making emerged as an important predictor of accountability ambiguity. Organizations experienced greater difficulty identifying responsibility when multiple actors possessed only partial control, knowledge, or visibility over digitally mediated decisions. The problem was particularly evident when algorithmic recommendations influenced managerial judgment, automated processes operated with limited interpretability, or external vendors controlled essential technical components. Legal responsibility did not necessarily disappear under these conditions, but the organizational pathway through which responsibility could be traced became more complex.

Governance safeguards substantially reduced these accountability risks. Board digital competence, human oversight, algorithmic transparency, auditability, internal controls, and regulatory preparedness were positively associated with greater accountability clarity. Organizations with stronger safeguards were better able to define decision rights, establish intervention thresholds, document technological influence, identify responsible actors, and respond when digital systems generated harmful or questionable outcomes. Technological complexity therefore did not inevitably produce accountability failure.

The findings support the proposed pathway of Digital Transformation - Distributed Decision-Making - Accountability Gap - Governance Safeguards - Legal Accountability. Digital transformation increased accountability risks primarily when technological influence expanded without equivalent improvements in oversight, traceability, and responsibility allocation. The central governance challenge is therefore not simply controlling technology but maintaining a defensible connection among formal authority, meaningful control, relevant knowledge, foreseeable risk, and the capacity to intervene.

The findings are consistent with established corporate-governance scholarship emphasizing accountability, transparency, monitoring, fiduciary responsibility, internal control, and effective board oversight. Traditional governance theory assumes that organizational authority can be attributed to identifiable actors who possess decision rights and corresponding responsibilities. Digital transformation complicates this assumption by introducing technological systems that influence decisions without possessing legal responsibility in the same institutional sense as corporate actors. The present findings extend conventional governance perspectives by demonstrating that accountability increasingly depends on how human authority is structured around technologically mediated decision processes.

The results also align with emerging scholarship on responsible artificial intelligence and algorithmic governance, which emphasizes transparency, explainability, human oversight, fairness, and auditability. The present study extends this literature by locating these principles within corporate governance structures rather than treating them solely as technical or ethical requirements. Algorithmic transparency becomes institutionally meaningful when it enables boards, managers, auditors, regulators, and affected stakeholders to understand relevant aspects of decision processes and identify where responsibility resides.

The findings differ from technologically deterministic interpretations suggesting that increasing automation necessarily produces an unavoidable responsibility gap. Automated systems can complicate causal attribution and reduce direct human involvement, but the case evidence demonstrates that organizations can preserve accountability through appropriate governance architecture. Human-review thresholds, documented decision rights, independent validation, audit trails, escalation mechanisms, and clearly assigned executive responsibility can maintain traceability even in technologically complex environments.

The results also qualify the assumption that outsourcing technological functions transfers corresponding responsibility to external providers. Third-party vendors may bear contractual, technical, or regulatory obligations, but corporations frequently retain responsibilities toward customers, employees, shareholders, regulators, and other stakeholders. The findings demonstrate that operational outsourcing may actually intensify accountability risks when corporations become dependent on systems they cannot adequately inspect, challenge, or control. Contractual allocation of responsibility is therefore not equivalent to effective governance accountability.

The findings signify that digital transformation should be understood as a transformation of corporate accountability architecture. Technology changes not only how organizations operate but also where information resides, how decisions are generated, who possesses expertise, and who can intervene when risks emerge. Governance systems designed around relatively centralized human decision-making may therefore become inadequate when operational influence is distributed across algorithms, technical teams, external vendors, and automated infrastructures.

The findings also signify an increasing separation between formal authority and operational influence. A board may retain ultimate oversight responsibility while lacking detailed knowledge of the algorithmic systems shaping corporate decisions. Technical teams may understand system behavior without possessing authority to determine broader corporate policy. External providers may control important technological components while having limited responsibility for the organizational consequences of their outputs. Accountability gaps emerge precisely where these forms of authority, knowledge, control, and responsibility become misaligned.

The positive role of board digital competence signifies that effective oversight in the digital era requires a new form of governance capability. Directors do not need to become software engineers or data scientists, but they require sufficient digital literacy to question assumptions, understand material technological risks, demand appropriate assurance, evaluate governance structures, and recognize circumstances requiring independent expertise. Digital competence should therefore be understood as an oversight capability rather than technical specialization.

The findings signify that legal accountability remains fundamentally human and institutional even when technology exercises substantial functional influence. Artificial intelligence may generate recommendations, classify individuals, detect patterns, or automate decisions, but organizations determine why systems are adopted, which data they use, how outputs are applied, what safeguards are implemented, and when human intervention is required. Technological

complexity may complicate responsibility attribution, but it should not automatically become a justification for accountability avoidance (Ibragimov, 2026; Pirannejad, 2026).

The primary implication for corporate governance is that boards should treat digital transformation as a governance issue rather than delegating it exclusively to information-technology departments. Board oversight should address strategic technological dependence, algorithmic risk, cybersecurity, data governance, third-party systems, automated decision-making, and potential stakeholder harm. Digital initiatives with material legal or social consequences require governance structures proportionate to their risk.

Corporations should establish explicit accountability maps for high-impact digital systems. Such maps should identify who authorizes deployment, who validates system performance, who monitors ongoing operation, who reviews contested outputs, who can suspend the system, and who bears executive responsibility for resulting decisions. Responsibility should be assigned before harm occurs rather than reconstructed retrospectively after a failure.

Legal and compliance functions should become more deeply integrated with digital-system governance. Compliance review conducted only after technological implementation may be insufficient because accountability risks can become embedded during system design, data selection, model procurement, and workflow integration. Legal accountability should therefore be incorporated throughout the technology lifecycle, from procurement and design to deployment, monitoring, modification, and retirement (Ahmed, 2025; Pirannejad, 2026).

Regulators and policymakers should avoid relying exclusively on abstract principles of responsible digital governance. Requirements for transparency, human oversight, and accountability become meaningful only when organizations can operationalize them through documentation, auditability, decision rights, intervention procedures, and enforceable duties. Regulation should therefore encourage demonstrable governance capabilities rather than symbolic compliance with broad ethical principles.

The relationship between digital transformation and distributed decision-making can be explained by the increasing specialization of contemporary corporate systems. Complex digital operations require expertise from managers, data scientists, software developers, compliance professionals, cybersecurity specialists, vendors, and automated systems. No single actor necessarily possesses complete knowledge of the entire decision chain. Organizational efficiency may increase through specialization, but responsibility becomes more difficult to trace when decision authority is not explicitly coordinated (Alhazmi, 2026; Karichalil, 2026).

The accountability gap becomes larger when organizations confuse technological reliance with responsibility transfer. Managers may defer to algorithmic outputs because systems are perceived as objective or technically sophisticated, while technical teams may view final decisions as managerial responsibilities. Vendors may consider themselves responsible only for system performance rather than organizational outcomes. Such fragmented perceptions create situations in which each actor can plausibly claim that another party controlled the decisive element.

Governance safeguards reduce these risks because they reconnect technological influence with organizational responsibility. Human oversight creates identifiable intervention points, auditability preserves evidence of how decisions were generated, transparency improves understanding of relevant system behavior, and internal controls define who must review or authorize particular actions. These mechanisms do not eliminate technological risk, but they make responsibility more traceable and contestable.

Board digital competence matters because governance quality depends partly on the capacity to recognize which questions require attention. A board that lacks sufficient understanding of digital

systems may receive extensive technical information without identifying material governance implications. Competent oversight enables directors to distinguish routine technological matters from issues involving significant legal exposure, stakeholder rights, strategic dependency, or systemic risk. Digital competence therefore improves accountability by strengthening the quality of institutional questioning and escalation (Eller, 2026; Wählich, 2026).

Future research should examine digital corporate accountability longitudinally rather than relying primarily on cross-sectional evidence. Accountability structures evolve as organizations gain experience with artificial intelligence and automated systems, while technological risks change as models, data, regulations, and business processes develop. Longitudinal studies could determine whether governance safeguards mature alongside digital transformation or whether accountability gaps persist as structural features of technologically complex corporations.

Future studies should compare accountability architectures across industries and regulatory jurisdictions. Financial services, healthcare, employment, manufacturing, and digital platforms involve different levels of automation, stakeholder vulnerability, regulatory scrutiny, and potential harm. Comparative research could identify which governance mechanisms are universally important and which require sector-specific adaptation (Lokeshwari, 2025; Wählich, 2026).

Future empirical research should investigate accountability following actual digital failures rather than relying solely on perceptions and formal policies. Case studies of algorithmic discrimination, cybersecurity incidents, automated financial decisions, data misuse, or AI-related operational failures could trace how responsibility is reconstructed after harm occurs. Such analysis would reveal whether formal accountability frameworks function effectively under real organizational pressure.

Future scholarship should move beyond asking “Who made the digital decision?” because technologically mediated corporate decisions rarely result from a single identifiable actor. A more rigorous accountability inquiry should ask who possessed formal authority, who exercised meaningful control, who had access to relevant knowledge, who could reasonably foresee the risk, who had the capacity to intervene, and who benefited from or authorized the underlying system. This approach can support a more mature model of corporate governance in which technological complexity does not dilute responsibility but instead requires more precise accountability architecture. Digital transformation should ultimately be judged not only by its capacity to increase efficiency and innovation, but also by whether corporations remain capable of explaining, auditing, contesting, and accepting responsibility for the decisions made through the digital systems they choose to deploy.

CONCLUSION

The most important finding of this study is that digital transformation does not inherently weaken corporate accountability; rather, accountability becomes vulnerable when technological influence expands faster than the governance structures designed to supervise it. Increasing reliance on artificial intelligence, automated systems, data analytics, and third-party digital providers distributes decision-making across multiple human and technological actors, creating gaps between formal authority, operational influence, technical knowledge, and responsibility. Organizations with stronger board digital competence, human oversight, algorithmic transparency, auditability, internal controls, and regulatory preparedness demonstrated greater clarity in tracing responsibility for digitally mediated decisions. The distinctive finding therefore lies in identifying the accountability gap as a problem of governance misalignment rather than technological autonomy. Artificial intelligence may substantially influence corporate decisions, but technological complexity does not

eliminate the responsibility of corporations and legally accountable actors for authorizing, deploying, supervising, auditing, and responding to the consequences of the digital systems they use.

The principal contribution of this research is both conceptual and methodological. Conceptually, the study advances a Digital Corporate Accountability Framework represented by Digital Transformation - Distributed Decision-Making - Accountability Gap - Governance Safeguards - Legal Accountability. The framework extends conventional corporate governance theory by connecting responsibility to five interrelated dimensions: formal authority, meaningful control, access to relevant knowledge, reasonable foreseeability of risk, and capacity to intervene. This perspective moves beyond the narrow question of who formally made a decision and provides a more realistic basis for attributing responsibility within complex human–technology systems. Methodologically, the integration of corporate governance surveys, comparative legal analysis, organizational document review, semi-structured interviews, and cross-case analysis provides a multidimensional approach for examining the relationship between formal legal obligations and actual governance practices. This contribution bridges corporate governance, digital regulation, and organizational accountability while providing an analytical foundation for evaluating whether corporate digitalization is accompanied by sufficiently robust accountability architecture.

The study is limited by its cross-sectional design, purposive organizational sampling, reliance on professional perceptions, selected regulatory contexts, and variation in technological maturity across participating corporations. These limitations restrict causal inference and may not fully capture how accountability structures evolve as technologies, regulations, and organizational practices change over time. Future research should employ longitudinal and multi-jurisdictional designs and examine actual cases involving algorithmic failures, automated discrimination, cybersecurity incidents, data misuse, and AI-related corporate harm to determine how responsibility is attributed under real conditions. Comparative studies should also investigate sector-specific differences and the effectiveness of board-level AI governance, algorithmic audits, human-oversight mechanisms, third-party accountability arrangements, and emerging regulatory regimes. Future scholarship should ultimately determine how corporate governance can ensure that increasing technological complexity strengthens rather than obscures responsibility, establishing accountability systems capable of identifying who had authority, who exercised meaningful control, who understood or should have understood the risk, who could intervene, and who must legally answer for the consequences of digitally mediated corporate decisions.

DECLARATION OF AI AND AI ASSISTED TECHNOLOGIES IN THE WRITING PROCESS

During the preparation of this work the author(s) used Google Assisted to assist in improving grammar, language quality, and overall readability of the text. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.

Author 2: Conceptualization; Data curation; Investigation.

Author 3: Data curation; Investigation.

Author 4: Formal analysis; Methodology; Writing - original draft.

Author 5: Supervision; Validation.

DECLARATION OF COMPETING INTEREST

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

REFERENCES

- Ababneh, J. (2025). Cybersecurity Ethical Aspects (CEA). *IEEE Access*, 13(Query date: 2026-07-23 21:53:18), 212443–212468. <https://doi.org/10.1109/ACCESS.2025.3641180>
- Ahdadou, M. (2026). From augmentation to autonomy: Artificial intelligence and the destabilization of agency in corporate governance. *Futures*, 182(Query date: 2026-07-23 21:53:18). <https://doi.org/10.1016/j.futures.2026.103873>
- Ahmed, M. M. (2025). The ethics of data mining in healthcare: Challenges, frameworks, and future directions. *Biodata Mining*, 18(1). <https://doi.org/10.1186/s13040-025-00461-w>
- Alhazmi, A. H. J. (2026). The CMA Agentic Platform: Autonomous Asset Verification and Algorithmic Auditor Governance. *Fintech*, 5(2). <https://doi.org/10.3390/fintech5020055>
- Aliaga, N. S. (2026). Beyond the algorithm: Cooperative alternatives to platform capitalism in urban delivery workforces. *Digital Geography and Society*, 10(Query date: 2026-07-23 21:53:18). <https://doi.org/10.1016/j.diggeo.2026.100157>
- Alyami, N. M. (2026). ETHICAL AND LEGAL ASPECTS OF DIGITAL MARKETING, INFORMATION TECHNOLOGY, AND THEIR INFLUENCE ON CORPORATE GOVERNANCE AND SUSTAINABLE DEVELOPMENT. *Corporate Law and Governance Review*, 8(2), 63–76. <https://doi.org/10.22495/clgrv8i2p6>
- Amayreh, M. S. (2026). Legal and Economic Perspectives under Malaysia's MADANI Framework: ESG, and AI. *2026 International Conference on Artificial Intelligence for Sustainable Engineering and Innovation Aisei 2026*, (Query date: 2026-07-23 21:53:18), 423–431. <https://doi.org/10.1109/AISEI68628.2026.11572892>
- Ayhan, U. (2025). Smart Cities and Control: Reconsidering Techno-Politics and Individual Agency in China and the UK. *Rethinking Techno Politics in the Digital Age Global Technology Relations and Security*, (Query date: 2026-07-23 21:53:18), 109–126. <https://doi.org/10.4018/979-8-3373-2459-3.ch004>
- Azer, M. A. (2024). Overview of the Complex Landscape and Future Directions of Ethics in Light of Emerging Technologies. *International Journal of Advanced Computer Science and Applications*, 15(7), 1459–1481. <https://doi.org/10.14569/IJACSA.2024.01507142>
- Balan, Y. (2025). Big Tech and the Myth of Transparency: Simulated Accountability and the Politics of Platform Governance. *Cultural Transformation and Disruption Through Media and Communication*, (Query date: 2026-07-23 21:53:18), 183–210. <https://doi.org/10.4018/979-8-3373-4089-0.ch006>
- Bohlens, C. (2025). Navigating AI and children's rights in corporate practices: Ethical AI integration in corporate responsibility. *Human Values Ethics and Dignity in the Age of Artificial Intelligence*, (Query date: 2026-07-23 21:53:18), 239–284. <https://doi.org/10.4018/979-8-3693-9035-1.ch011>
- Bose, V. (2026). Managing People and Algorithms: Corporate Responsibility and Human Resource Management Perspective on AI Adoption. *Rethinking Responsibility at the Intersection of AI and Corporate Liability*, (Query date: 2026-07-23 21:53:18), 261–288. <https://doi.org/10.4018/979-8-3373-6390-5.ch011>
- Bressane, A. (2026). Corporate environmental intelligence as an emerging governance framework in digital sustainability: A scoping review. *Environmental Development*, 59(Query date: 2026-07-23 21:53:18). <https://doi.org/10.1016/j.envdev.2026.101467>
- Canato, M. C. (2026). From ethics washing to enforceable accountability: Hospitals as hubs of digital constitutionalism. *AI and Society*, (Query date: 2026-07-23 21:53:18). <https://doi.org/10.1007/s00146-026-02980-4>

- Cicu, G. C. (2024). Bridging Traditional Corporate Governance and Technology: The ‘AI Corporate Design’ Framework to Computational Corporate Governance Model. *Italian Law Journal*, 10(1), 345–362.
- Cowin, J. (2025). Autonomous AI Agents The Kraken Wakes. *Proceedings Imcic International Multi Conference on Complexity Informatics and Cybernetics*, (Query date: 2026-07-23 21:53:18), 20–23. <https://doi.org/10.54808/IMCIC2025.01.20>
- Eller, K. H. (2026). The “Digital Turn” of Value Chain Due Diligence Regulation: How Technology Reconfigures Stakeholder Engagement. *Global Policy*, (Query date: 2026-07-23 21:53:18). <https://doi.org/10.1111/1758-5899.70165>
- Gkasis, P. (2026). Beyond Borders: The Quest for a Global Business Ethic. *Ethics in the Modern Business Environment*, (Query date: 2026-07-23 21:53:18), 153–158. <https://doi.org/10.4324/9781003647980-27>
- Hinov, N. (2026). LLM-Augmented Algorithmic Management: A Governance-Oriented Architecture for Explainable Organizational Decision Systems. *AI Switzerland*, 7(3). <https://doi.org/10.3390/ai7030102>
- Ibragimov, A. (2026). The Role of Algorithmic Fiduciaries in Decentralized Autonomous Organizations and the Assignment of Duty and Developer Liability for Autonomous Smart Governance. *Indian Journal of Information Sources and Services*, 16(2), 311–318. <https://doi.org/10.51983/ijiss-2026.16.2.31>
- Ishkhanyan, A. (2026). Governing AI across borders: Corporate power, state sovereignty and global regulation. *Digital Policy Regulation and Governance*, 28(3), 280–295. <https://doi.org/10.1108/DPRG-03-2025-0057>
- Ismail, O. (2025). Ethical and Governance Frameworks for Artificial Intelligence: A Systematic Literature Review. *International Journal of Interactive Mobile Technologies*, 19(14), 121–136. <https://doi.org/10.3991/ijim.v19i14.56981>
- Karichalil, R. A. (2026). The Emancipation Paradox: When AI-Enhanced Personalization Undermines Consumer Agency and What Socially Responsible Marketing Requires. *Journal of Macromarketing*, (Query date: 2026-07-23 21:53:18). <https://doi.org/10.1177/02761467261447188>
- Khalil, M. K. (2026). Digital Governance in the ESG Era: Enhancing Transparency, Accountability, and Sustainability. *Digital Evolution of Esg 3 0 Advancing Corporate Governance and Sustainability*, (Query date: 2026-07-23 21:53:18), 17–32. <https://doi.org/10.1108/978-1-83662-758-620261002>
- KRAFZIK, S. (2026). CORPORATE GOVERNANCE AND ARTIFICIAL INTELLIGENCE: THE EMERGING LEGAL CHALLENGES IN SOUTH AFRICA’S BOARDROOMS. *South African Law Journal*, 143(2), 251–282. <https://doi.org/10.47348/SALJ/v143/i2a3>
- Kunz, W. H. (2026). CORPORATE DIGITAL RESPONSIBILITY IN TOURISM AND HOSPITALITY: Ethical Challenges and Strategies for AI Implementation. *Ethics of AI in Hospitality and Tourism Challenges and Opportunities*, (Query date: 2026-07-23 21:53:18), 57–71. <https://doi.org/10.4324/9781003643951-4>
- Lokeshwari, R. (2025). Social and Ethical Challenges of Artificial Intelligence in Surveillance and Security Systems. *2025 9th International Conference on Computational System and Information Technology for Sustainable Solutions Csitss 2025*, (Query date: 2026-07-23 21:53:18). <https://doi.org/10.1109/CSITSS67709.2025.11294538>
- Mamilla, J. L. K. (2025). Digital Tools and Data-Driven Accountability: Enhancing Directors’ Oversight of CSR Through Technology. *Investigating Directors Accountability in Promoting Corporate Social Responsibility*, (Query date: 2026-07-23 21:53:18), 247–274. <https://doi.org/10.4018/979-8-3373-3695-4.ch009>
- Manoharan, S. (2026). Corporate Governance in the Age of Algorithmic Human Resource Management: Directors’ and Officers’ Oversight of Artificial Intelligent Systems. *Rethinking Responsibility at the Intersection of AI and Corporate Liability*, (Query date: 2026-07-23 21:53:18), 237–260. <https://doi.org/10.4018/979-8-3373-6390-5.ch010>

- Naz, A. (2026). Enhancing Diversity, Equity, and Inclusion Through Digital Initiatives in ESG in Corporate Governance. *Digital Evolution of Esg 3 0 Advancing Corporate Governance and Sustainability*, (Query date: 2026-07-23 21:53:18), 137–163. <https://doi.org/10.1108/978-1-83662-758-620261009>
- Nosikov, A. (2026). Metaverses and Public Policy: Prospects for Virtual Civic Participation. *Communications in Computer and Information Science*, 2671(Query date: 2026-07-23 21:53:18), 380–393. https://doi.org/10.1007/978-3-032-04958-2_28
- Okuno, M. J. (2025). Legal frameworks for AI service business participants: A comparative analysis of liability protection across jurisdictions. *AI and Society*, 40(7), 5667–5683. <https://doi.org/10.1007/s00146-025-02288-9>
- Perrier, E. (2026). Operationalising Extended Cognition: Formal Metrics for Corporate Knowledge and Legal Accountability. *Cslaw 2026 Proceedings of the 2026 Symposium on Computer Science and Law*, (Query date: 2026-07-23 21:53:18), 210–225. <https://doi.org/10.1145/3788646.3789534>
- Pirannejad, A. (2026). The evolution of HR governance: A systematic review and integrative framework for future research. *Human Resource Management Review*, 36(3). <https://doi.org/10.1016/j.hrmr.2026.101150>
- Schuessler, E. (2026). Digital platforms and democratic publics: How social media platforms selectively appropriate and strategically subvert institutional logics. *Information and Organization*, 36(1). <https://doi.org/10.1016/j.infoandorg.2026.100612>
- Sharma, G. K. (2025). Ethical considerations in the use of AI and big data in corporate decision-making. *Digital Citizenship and the Future of AI Engagement Ethics and Privacy*, (Query date: 2026-07-23 21:53:18), 467–531. <https://doi.org/10.4018/979-8-3693-9015-3.ch017>
- Singh, D. (2025). Corporate Governance and AI Ethics: Strategic Framework for Ethical Decision-Making in Business. *International Conference on Intelligent and Innovative Practices in Engineering and Management Iipem 2025*, (Query date: 2026-07-23 21:53:18). <https://doi.org/10.1109/IIPEM65914.2025.11548042>
- Taşkale, A. R. (2026). Manufacturing the Leviathan: Palantir’s ‘Technological republic’ and the nationalist faction of the tech oligarchy. *Science as Culture*, (Query date: 2026-07-23 21:53:18). <https://doi.org/10.1080/09505431.2025.2607360>
- Torralba, M. H. (2026). Interpretability and the Measurement of Ethical Foundations in Artificial Intelligence. *Lecture Notes in Computer Science*, 15939(Query date: 2026-07-23 21:53:18), 27–34. https://doi.org/10.1007/978-3-032-01429-0_3
- Toukabri, M. (2025). Evolution of Corporate Accountability for Biodiversity Reporting. Do Stakeholder Capitalism and Institutional Context Matter? A Bibliometric Analysis. *Business Strategy and Development*, 8(2). <https://doi.org/10.1002/bsd2.70095>
- Vartiak, L. (2025). Silicon Forests: How AI Is Regreening the Corporate Landscape. *Generative AI for A Net Zero Economy Managing Climate Change and Business Innovation in the Digital Era*, (Query date: 2026-07-23 21:53:18), 19–36. https://doi.org/10.1007/978-981-96-8015-3_2
- Wählisch, M. (2026). Structural dilemmas of PeaceTech: AI, power, and peacebuilding in the digital age. *Peacebuilding*, (Query date: 2026-07-23 21:53:18). <https://doi.org/10.1080/21647259.2026.2644694>
- Yazici, C. O. (2026). Compliance in Digital Environments: Integrating RegTech into Governance, Risk and Compliance. *2026 Innovations in Machine Engineering and Digital Conference Imed 2026*, (Query date: 2026-07-23 21:53:18). <https://doi.org/10.1109/IMED68921.2026.11484469>
- Yigitcanlar, T. (2026). Governing Urban AI from the Frontline: A Stage-Gate Framework for Municipal Algorithmic Decision-Making. *Smart Cities*, 9(5). <https://doi.org/10.3390/smartcities9050081>

Copyright Holder :

© Dodi Rusmana et al. (2026).

First Publication Right :

© Rechtsnormen Journal of Law

This article is under:

