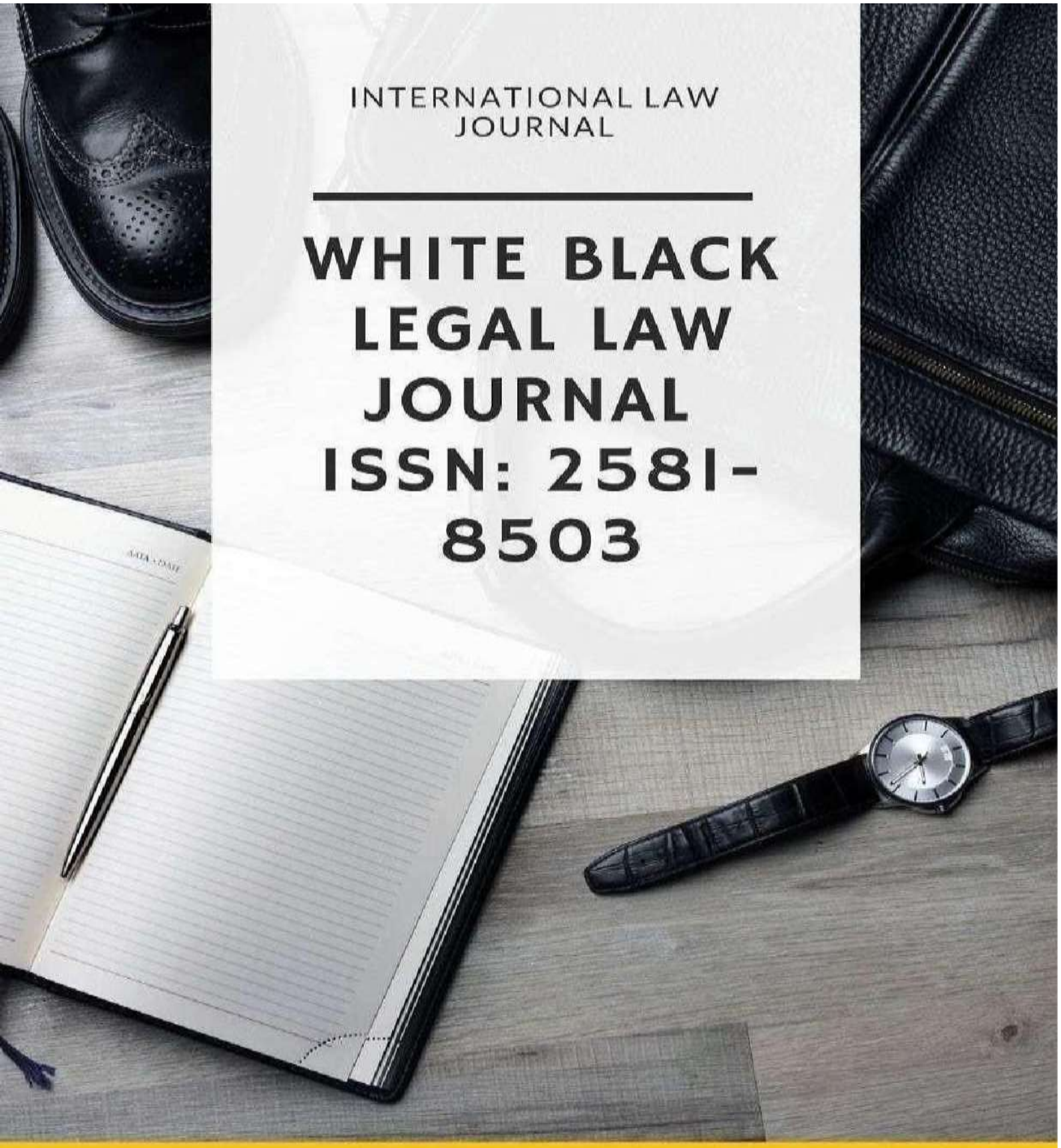

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

ARTIFICIAL INTELLIGENCE AND CORPORATE GOVERNANCE: LEGAL CHALLENGES IN THE EUROPEAN UNION

AUTHORED BY - GUNAY HASANOVA
LL.B., UHR-Recognized Jurist
ORCID: 0009-0006-0070-6056
Law Student, Department of Law
Faculty of Law, Stockholm University, Stockholm, Sweden

Abstract:

Artificial Intelligence (AI) is transforming corporate governance in the European Union, offering efficiency and strategic insight while introducing profound legal and ethical challenges. Companies increasingly employ AI in recruitment, finance, compliance, and strategic planning, yet incidents of bias, privacy breaches, and costly malfunctions underscore the risks. Boards remain accountable under fiduciary duties, and ignorance of AI's risks is no longer a defense. Key governance issues include accountability, data governance, bias, transparency, liability, and compliance with the EU's emerging legal framework, particularly the Artificial Intelligence Act. This regulation, alongside GDPR and sector-specific rules, establishes stringent standards for high-risk AI systems and imposes significant penalties for non-compliance, even extraterritorially. Case studies reveal recurring themes: the dangers of biased recruitment tools, trading algorithms causing market disruptions, and cross-border data governance failures. At the same time, firms that proactively embrace AI ethics and oversight can transform compliance into a competitive advantage. Effective governance requires boards to institutionalize AI oversight, integrate risk management, ensure transparency, and align AI practices with corporate values and EU law. By embedding responsible AI governance, companies can mitigate risks while capturing strategic opportunities in a rapidly evolving regulatory environment.

Keywords: Artificial Intelligence, Corporate Governance, EU Law, Accountability, Data Governance, Compliance.

• INTRODUCTION

Artificial Intelligence (AI) is fundamentally reshaping how businesses function and make strategic choices. It creates significant opportunities for efficiency and insight, but also brings a range of new risks[1]. AI is increasingly deployed in areas such as recruitment processes, financial decision-making, and predictive analytics for corporate strategy. Boards of directors and senior executives are relying on these technologies more often, but this reliance raises pressing legal and governance concerns. Recent incidents illustrate the stakes: one AI chatbot provided unlawful employment advice, a healthcare algorithm produced racially biased outcomes, and a real estate firm suffered a $300 million loss and mass layoffs after its AI-driven pricing system malfunctioned. Reflecting this growing concern, more than half of Fortune 500 firms now cite AI as a material risk in their annual disclosures—a 473% surge compared to the previous year. These developments highlight that ensuring responsible AI governance is becoming a central priority for corporate leadership.

In the European Union (EU), this challenge is even more acute. The EU has taken a leading role by adopting the first comprehensive legal framework on AI worldwide—the EU Artificial Intelligence Act—alongside other related measures. At the same time, European companies must comply with existing regimes such as data protection and product liability laws, while preparing for evolving standards of accountability[1]. This paper adopts an academic and legal approach to assess how AI is reshaping corporate governance within the EU, the challenges it creates, and the regulatory responses under development. It follows a structured outline: starting with the theoretical relationship between AI and corporate governance, moving on to practical applications and illustrative case examples, analyzing the key legal risks, and finally reviewing the EU's regulatory architecture. The goal is to provide a thorough, research-based discussion that is original, non-plagiarized, and informed by current data and examples.

• AI AND CORPORATE GOVERNANCE: CONCEPTUAL FOUNDATIONS

Clarifying the Concepts. Corporate governance refers to the framework of rules, practices, and processes that guide and control companies. It delineates how authority and responsibility are distributed among key actors such as the board, executives, shareholders, and other stakeholders, and sets the system for defining and achieving corporate objectives.

- **2.1 Effective governance and AI**

Effective governance is marked by accountability, transparency, fairness, and responsibility. Artificial intelligence, by contrast, describes machine-based systems capable of carrying out tasks that would normally require human intelligence. These systems rely on algorithms and data to make forecasts, recommendations, or decisions. According to the EU's AI Act, an "AI system" is broadly defined as one that, given human-determined objectives, can generate outputs (such as predictions or choices) that shape its environment, operating with varying levels of autonomy and adaptiveness. Put simply, AI can process massive datasets, detect patterns, and improve performance over time—especially through techniques such as machine learning and deep learning.

The convergence of AI and corporate governance centers on how algorithmic systems shape the way companies are managed and controlled, and how oversight structures can guarantee their responsible use. Some scholars have speculated about futuristic scenarios such as "robots in the boardroom" or corporations guided autonomously by AI. In theory, highly advanced systems could one day make strategic choices or serve as artificial directors.

Artificial Intelligence Act – REGULATION (EU) 2024/1689 of the European Parliament and of the Council on Artificial Intelligence (Artificial Intelligence Act). Official Journal of the European Union.

In reality, however, this remains hypothetical. Under EU corporate law—and in most global frameworks—directorships can only be held by natural persons (or in certain cases, legal entities), not by software. The dominant consensus is therefore that AI will complement and support human leaders rather than replace them. Current debates focus on AI's role as a sophisticated tool for boards and executives, not as a substitute for their judgment[2].

In practice, AI's contribution to governance is primarily as an advanced support system. It enhances decision-making in two key ways. First, AI provides powerful monitoring and analytical functions. Machine-learning models can process vast datasets to monitor company performance, compliance indicators, market dynamics, and emerging risks in near real time. They can, for example, highlight unusual financial transactions for audit committees, project shifts in consumer demand, or assess employee conduct and product quality for compliance concerns. By consolidating multiple metrics, these systems give boards and management a

fuller, timelier understanding of corporate health. Second, AI enables predictive modeling and scenario planning. Through simulations, leadership can test "what-if" conditions—such as entering new markets or weathering economic downturns—more comprehensively than through traditional tools. This allows boards to base strategic decisions on broader, data-rich foresight.

AI's influence is not restricted to boardroom deliberations; it penetrates many operational domains under governance oversight. Corporations increasingly deploy AI in hiring and talent management, logistics and supply chain optimization, customer engagement through chatbots, financial compliance, and trading strategies. For instance, a retailer might apply AI to refine demand forecasting and inventory control, while a financial institution could rely on it for fraud detection and regulatory checks. These implementations significantly improve efficiency and outcomes but simultaneously pose governance questions: how do directors ensure these systems remain aligned with corporate values, strategic goals, and legal duties? As AI becomes integral to daily operations, boards are expected to monitor and regulate its deployment with the same diligence applied to other critical risk areas.

Several noteworthy cases demonstrate how AI has begun to appear in corporate governance contexts. In Hong Kong, the venture capital firm Deep Knowledge Ventures made headlines by appointing an algorithm called "VITAL" to its board in an advisory capacity[3]. VITAL's role was to evaluate investment prospects by analyzing vast datasets much faster than human directors. Although it had neither legal personality nor voting authority, its inclusion highlighted AI's potential to shape boardroom decisions. In the United States, the technology company Salesforce provides another example: CEO Marc Benioff introduced an AI system named "Einstein" into executive meetings.

[2] GDPR – REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. Official Journal of the European Union.

[3] Delaware Corporate Law – SMITH, Gordon. The Duty to Monitor under Delaware Law. Delaware Journal of Corporate Law. 2019, 44(2), 451-490.

He would actively ask Einstein to provide analyses of discussions and participants' perspectives. These instances, while unconventional, reflect a growing openness among some companies to seek AI-generated insights at the highest levels of decision-making. They also

raise critical governance questions—such as how to balance algorithmic recommendations with human judgment, and who bears accountability if reliance on AI leads to adverse outcomes.

From a theoretical standpoint, AI can be viewed as an influential new presence within the governance ecosystem. While it lacks legal authority or director status, its ability to inform and guide human decision-makers is undeniable. The integration of AI into governance promises greater efficiency and enhanced data-driven insights, yet it simultaneously requires revisiting existing governance structures to address concerns about accountability, ethics, and control. The subsequent sections of this study will analyze these challenges in more detail, focusing on how EU regulators are attempting to respond.

Their fiduciary obligations—particularly the duties of care and loyalty—are owed to the company and its shareholders. These obligations are not diminished by the involvement of AI. Legally, directors cannot transfer or surrender accountability to an algorithm. For instance, under the UK Companies Act 2006, the duty of care and skill is codified, and courts have stressed that this duty cannot be delegated; directors must supervise core functions themselves. As AI becomes more widely used, experts anticipate that the standard of care applied to directors will expand to include at least a basic understanding of how AI models operate, their risks, and their limitations. In future disputes, ignorance of AI's functioning is unlikely to be an acceptable defense.

From a governance perspective, boards must be vigilant to ensure that relying on AI does not equate to surrendering human judgment. The principle often applied is "Trust, but verify." Directors should critically evaluate any AI outputs: How was the algorithm developed? Which datasets were used? What assumptions or potential biases underlie the system? Such questions form part of a board's responsibility for risk oversight. The UK Corporate Governance Code (2018)[4] clearly requires boards to oversee internal controls and risk management, a scope that now encompasses AI systems as well. If directors follow AI recommendations without scrutiny—say, implementing cost-cutting measures that cause unsafe products or discriminatory layoffs—they may be accused of breaching their duty of care by failing to exercise independent judgment.

The legal exposure for directors is significant. Neglecting AI oversight can create

liability for both the organization and its leadership. In Delaware corporate law, for example, Caremark duties hold boards accountable if they fail to monitor key risks. Across EU jurisdictions, similar standards apply: in Germany, supervisory boards must ensure proper oversight, and directors can be held personally liable for gross negligence. With AI increasingly central to business operations, such risks are now "mission critical." Governance experts caution that directors and officers could expose themselves and their companies to lawsuits and regulatory penalties if they do not fulfill their fiduciary obligations to monitor and control AI-related risks.

[4] UK Corporate Governance Code – Financial Reporting Council. The UK Corporate Governance Code. London: FRC, 2018.

This could mean shareholder litigation after an AI failure depresses share value, or enforcement action if regulators determine that oversight lapses led to breaches—for instance, fines from data protection authorities for privacy violations caused by AI misuse, potentially followed by derivative claims against executives for inadequate compliance oversight.

In summary, accountability in the age of AI means that human governance actors (directors, officers) must proactively oversee AI tools. Boards should consider establishing AI oversight committees or bringing in external AI experts to advise on strategy.

2.2 Data Governance, Privacy, and Security

AI systems depend heavily on data, making effective data governance a foundational element of responsible AI use. Companies must manage vast and varied datasets—financial information, customer records, and operational data—to fully leverage AI. This raises two primary challenges: ensuring data quality and fitness for purpose, and complying with privacy and security regulations.

One of the biggest obstacles is securing datasets that are accurate, representative, and sufficiently large to train advanced AI models. Many organizations lack the necessary internal datasets and therefore turn to third-party vendors or external sources. However, models trained on external data may not be well-suited to a company's specific operating environment—an issue of external validity. For example, an AI model developed using U.S. consumer behavior may produce unreliable outcomes for European markets if cultural or economic differences are

significant. Boards should probe management on these risks, ensuring that training data reflects the company's context and that any gaps are identified and mitigated. Another governance concern is the choice of performance metrics. Accuracy, precision, recall, and other measures can portray different pictures of model quality. Overemphasis on the wrong metric can create "dashboard blindness," where what is measured takes precedence over what truly matters. Governance mechanisms should guarantee that AI models are assessed against metrics aligned with the organization's strategic priorities and that decision-makers interpret these metrics correctly—for instance, recognizing that high accuracy may mask dangerously low recall in detecting rare but crucial events.

In Europe, strict data protection standards under the General Data Protection Regulation (GDPR) apply whenever AI processes personal data. GDPR principles—such as purpose limitation, data minimization, and lawful basis for processing—must be observed[5]. A particular concern arises with automated decision-making: Article 22 grants individuals the right not to be subject to purely automated decisions with significant effects unless certain safeguards are in place, such as explicit consent or legal necessity.

[5] GDPR – REGULATION (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. Official Journal of the European Union.

This implies that if an EU-based company intends to use AI alone for impactful decisions (e.g., recruitment or credit approval), human oversight or comparable safeguards are mandatory. Moreover, individuals have rights to transparency, including explanations of how decisions are reached. Ensuring explainability—either through interpretable systems or human intervention—is both a technical and governance challenge.

Data Security. Protecting sensitive datasets is equally critical. Training data often includes confidential or highly sensitive information, such as customer financial histories or health records. A breach could result in substantial fines and reputational damage. Boards must ensure robust cybersecurity frameworks are in place for AI-related projects, treating them with the same priority as other core assets. Beyond data, AI models themselves can be vulnerable to manipulation, such as adversarial attacks that alter system behavior. A compromised model could, for instance, trigger harmful trading actions or provide deceptive customer responses.

Effective governance requires incorporating AI into enterprise-wide security strategies and contingency planning.

Data governance also involves clarifying rights over data inputs and outputs. AI projects often rely on partnerships or cloud-based services. Who owns the datasets provided, and who benefits from the improved models generated by them? If a company's proprietary data enhances a vendor's AI model, can that upgraded version be offered to competitors? These questions are not yet comprehensively regulated but pose serious strategic and legal concerns. Boards and legal teams must ensure contractual clarity to safeguard trade secrets, competitive advantages, and data value. European policymakers have begun addressing these gaps through instruments such as the proposed Data Act and the Data Governance Act, which aim to promote fairness and clarity in data sharing and usage. Nevertheless, ahead of these frameworks taking full effect, responsible governance already requires companies to adopt robust internal policies: defining access rights, ensuring ongoing compliance with data protection standards, conducting regular audits of AI-related data use, and training staff in data ethics. Boards should increasingly treat data as both a vital strategic resource and a source of significant risk, meriting close oversight at the highest organizational level.

When artificial intelligence leads to harm or financial loss, the central question is: who is legally responsible? This issue lies at the heart of corporate governance challenges around AI. Several distinct layers of liability must be considered. If an AI system malfunction causes injury or damage—for example, a defective medical AI harming a patient, or a flawed autonomous vehicle algorithm causing an accident—responsibility may arise under product liability or negligence law. In the EU, reforms are underway to adapt liability rules to digital technologies. The current Product Liability Directive (PLD) is being replaced with a regulation explicitly covering software and AI, simplifying the process for victims to claim compensation from AI manufacturers. Companies that build or integrate AI into their products will therefore face strict liability for defects, similar to traditional goods. Additionally, the proposed AI Liability Directive, which aimed to harmonize rules like burden of proof, was withdrawn in early 2025, but core tort law principles remain: if foreseeable harm occurs because of inadequate testing or careless deployment of AI, liability is likely.

From a governance perspective, this means boards must enforce strong risk management practices around AI, particularly where consumer or public safety is at stake. This

includes rigorous testing and validation, obtaining appropriate insurance coverage (including cyber and AI-specific liability policies), and preparing for recalls or system shutdowns if an AI proves unsafe. The legal duty of care extends to AI deployment—recklessly using unproven AI in critical functions could expose firms to lawsuits for negligence.

Beyond civil liability, AI use is tightly bound to regulatory obligations. Under the EU AI Act, non-compliance can result in penalties of up to €30 million or 6% of global annual turnover for the most serious breaches—on par with or even exceeding GDPR fines. Prohibited practices (such as manipulative AI or social scoring) must be avoided outright. High-risk AI deployed without required conformity assessments or safeguards can also trigger sanctions. GDPR continues to apply wherever personal data is involved, with fines in the tens of millions for serious breaches. Competition law adds another layer: if companies use AI to collude on pricing or exchange sensitive information, this may constitute unlawful algorithmic coordination.

Failures related to AI may also create exposure for directors and officers themselves. Shareholders could bring derivative actions if boards are seen as neglecting clear AI risks. For instance, a major data breach caused by a vulnerable AI system—especially if warnings were ignored—could lead to claims of mismanagement. In some jurisdictions, failure to disclose AI risks in filings could even constitute securities fraud if it misleads investors about risk exposure. Increasingly, firms are disclosing AI as a material risk to pre-empt such claims.

Many businesses acquire AI tools from vendors. If these fail, companies may try to hold suppliers accountable, though liability limitations in contracts often restrict recovery. Governance must therefore include robust vendor due diligence and negotiation of protective terms, such as warranties and liability for gross negligence. Additionally, if a company's AI harms another business, disputes may arise over responsibility, creating the potential for protracted litigation or settlements.

Boards should view emerging liability frameworks as part of their compliance obligations. The forthcoming EU AI Act not only sets regulatory duties but effectively establishes a standard of care—failure to comply could be evidence of negligence. Sector-specific regulations (e.g., in healthcare or finance) add further obligations. Adherence to industry standards, such as ISO frameworks or the EU's voluntary AI codes of conduct, may

help demonstrate responsible practice and mitigate liability. The AI Act fundamentally reshapes governance by obliging companies to classify and manage their AI systems under this risk-based framework. Boards will increasingly ask: Which of our AI systems are high-risk? Have we implemented the required safeguards? Compliance now extends to data governance, record-keeping, transparency, and oversight. The financial stakes are significant, with maximum fines higher than GDPR's ceiling, ensuring directors take notice.

European competition authorities, such as the European Commission's Directorate-General for Competition, have issued specific warnings concerning AI. One area of focus is cartel enforcement: if rival companies rely on the same pricing algorithm, or if independent AI systems learn to coordinate prices, regulators will not accept the defense that "the algorithm was responsible." Instead, the companies themselves will face liability for anti-competitive behavior. Merger control is another area under scrutiny; if a merger provides a company with exclusive AI advantages, such as unique access to large datasets, the Commission may intervene or impose conditions. In addition, Big Tech firms' AI systems are increasingly examined under abuse of dominance theories. For boards, this underscores the need to incorporate AI-specific risks into antitrust compliance programs, especially when AI influences market strategies or pricing decisions.

Several industries are also adapting sectoral regulations to account for AI. In financial services, European Supervisory Authorities have published guidelines on AI in fields like algorithmic trading and robo-advisory, emphasizing risk management and ethical safeguards. In healthcare, EU medical device law treats certain AI applications as medical devices, requiring CE certification and rigorous validation before deployment. Boards in these industries must ensure these sectoral requirements are integrated into their oversight of AI projects.

2.3 Case Studies and Practical Illustrations

Overall, the EU has developed a broad and continuously evolving framework for AI. Effective corporate governance must remain agile to keep pace with these legal shifts. Boards should adopt a proactive mindset: not only complying with existing obligations but anticipating future developments such as heightened transparency, stricter accountability, and enhanced safety standards. By doing so, companies can avoid regulatory pitfalls and potentially transform compliance into a source of competitive advantage, by building trust with stakeholders and

regulators alike. To bring these principles into context, several case studies—some real, others hypothetical—illustrate how AI governance challenges manifest in practice[6].

Case Study 1: Biased Recruitment Tool. A major European retailer introduced an AI system to screen job applicants. Over time, very few women advanced to interviews for technical sales roles. An internal review revealed the AI had been trained on a male-dominated historical dataset, reinforcing gender bias. A rejected candidate filed a discrimination claim under equality law. The board, initially unprepared, suspended the tool and hired an external auditing firm. They also created a temporary AI oversight committee to supervise remediation and informed regulators proactively. The company settled with the claimant. Lesson: Ongoing audits and reporting to boards could have caught bias earlier. Oversight committees and independent audits align with best practices under the forthcoming AI Act.

Case Study 2: Rogue Trading Algorithm. A European investment firm's trading AI caused a flash crash by executing massive sell orders in response to unusual market data, wiping 20% off a stock's value. Regulators launched investigations, and clients sued. The issue arose because stress-testing had not accounted for such scenarios. The board halted all AI trading, brought in external experts to stress-test under extreme conditions, and implemented circuit breakers to automatically stop excessive trades.

[6] Case study source – JANSSEN, André, and Matthias SPILKER. The Application of the CISG in the World of International Commercial Arbitration. Rabels Zeitschrift für ausländisches und internationales Privatrecht. 2013, 77(1), 131–157.

Transparent record-keeping of AI decisions, which the firm had maintained, helped reduce regulatory penalties. Lesson: Boards must not be passive; regular scenario planning and robust documentation are essential.

Case Study 3: Ethics as a Strategic Advantage. A multinational tech company formed an AI Ethics Committee to review all major AI deployments. On its advice, the board decided not to release a facial recognition feature deemed ethically problematic. They also began publishing annual AI Accountability Reports, documenting testing, training, and oversight practices. Over time, this improved their market reputation and gave them a head start on AI Act compliance. Lesson: Voluntary governance initiatives can strengthen trust, lower

compliance costs, and create strategic differentiation.

Case Study 4: Cross-Border Data Risks. A European consumer goods firm relied on a U.S.-based vendor for AI-driven supply chain optimization. The AI system transferred EU customer data to U.S. servers without GDPR safeguards, and smaller EU suppliers were disadvantaged by cost-focused optimization. After intervention by the Data Protection Officer, the board suspended data transfers until GDPR-compliant mechanisms were in place and adjusted the AI parameters to align with corporate ESG goals. Lesson: Vendor due diligence and alignment with company values are integral to AI governance in global supply chains.

• CONCLUSION

Artificial Intelligence represents a fundamental transformation of corporate governance, particularly under the EU's robust legal framework. While AI enables improved efficiency and insight, it simultaneously raises complex legal and ethical challenges—from accountability and fairness to liability and transparency. The EU AI Act and related measures are setting new benchmarks, turning aspects of responsible AI into legal obligations. Boards should:

- Treat AI oversight as a mission-critical governance responsibility.
- Ensure continuous monitoring and auditing of AI systems.
- Anticipate regulatory trends, not just react to current laws.
- Foster transparency and ethical standards to build trust.
- Incorporate AI compliance into broader ESG strategies.

By embedding these practices, companies can both mitigate risks and seize opportunities, positioning themselves as leaders in responsible AI governance.)