JOURNAL OF MULTIDISCIPLINARY SCIENCES AND INNOVATIONS
VOLUME 5, ISSUE 04
MONTHLY JOURNALS
ISSN NUMBER: 2751-4390
IMPACT FACTOR: 9,08

REGULATING ARTIFICIAL INTELLIGENCE IN CORPORATE GOVERNANCE: A COMPARATIVE OVERVIEW OF THE UNITED STATES, THE EUROPEAN UNION, AND UZBEKISTAN

Nuriddin Khudoyberdiev
LL.M., Penn State Law, The Pennsylvania State University, USA; LL.M. and LL.B., Tashkent State University of Law, Uzbekistan.
n.khudoyberdiev.law@gmail.com

Abstract

Artificial intelligence is reshaping corporate decision-making, internal control, and disclosure practices across every major economy. Yet the legal frameworks that govern how companies deploy AI in their governance structures diverge sharply between jurisdictions. This article offers a concise comparative overview of three contrasting approaches. The United States has produced a layered and decentralized regime built on voluntary federal standards, sectoral securities regulation, and competing state statutes, recently overlaid by an executive-branch push for federal preemption. The European Union has adopted a horizontal and risk-based regulation in the AI Act of 2024, supplemented by the General Data Protection Regulation and the November 2025 Digital Omnibus simplification package. Uzbekistan has moved rapidly from strategic planning under Presidential Resolution PP-358 of October 2024 to a comprehensive AI law approved by the Senate in November 2025, but a number of corporate-governance gaps remain. After mapping each regime, the article distills six general recommendations for Uzbek reform, focused on risk classification, board-level oversight, disclosure, developer-deployer liability, institutional capacity, and international alignment.

Keywords: artificial intelligence; corporate governance; comparative law; EU AI Act; NIST AI Risk Management Framework; Uzbekistan AI Strategy 2030; algorithmic accountability; board oversight; risk-based regulation.

1. Introduction

In the space of three years, artificial intelligence has moved from an experimental decision-support tool to a core operational input in corporate governance. Boards now rely on AI for screening hiring pipelines, scoring credit applications, detecting fraud, monitoring compliance, drafting disclosures, and structuring strategic acquisitions. The legal question is no longer whether to regulate the corporate use of AI but how to regulate it without freezing innovation or shifting risk onto unprepared markets.

Three jurisdictions illustrate the principal regulatory choices that any country, including Uzbekistan, must make. The United States represents a layered and decentralized model: voluntary federal standards combined with sectoral regulation (especially in securities), state statutory experiments, and a recent federal push toward preemption. The European Union represents a horizontal and risk-based model centered on the AI Act of 2024 and reinforced by the General Data Protection Regulation. Uzbekistan represents a state-led model in which strategic planning has so far outpaced detailed legal rules.

This article maps the three regimes, places them side by side, and proposes six general recommendations for Uzbek reform. The argument is comparative rather than prescriptive:

Uzbekistan need not choose between American and European templates, but should select the elements of each that match its institutional capacity and economic ambitions.

2. Methods and Materials

The study uses a doctrinal and comparative legal method. Primary materials include the EU AI Act (Regulation 2024/1689), the General Data Protection Regulation, the Digital Omnibus on AI of November 19, 2025, the U.S. Blueprint for an AI Bill of Rights of October 2022, the NIST AI Risk Management Framework version 1.0 of January 2023, Executive Order 14365 of December 11, 2025, the White House National Policy Framework for Artificial Intelligence of March 20, 2026, Colorado Senate Bills 24-205 and 26-189, the Uzbek Presidential Resolution PP-358 of October 14, 2024, Cabinet of Ministers Resolution No. 425 of 2025, and the Uzbek AI Law approved by the Senate of the Oliy Majlis at its eleventh plenary session on November 1, 2025. Secondary materials include reports by the Council of the European Union, the European Parliament, the U.S. Securities and Exchange Commission Investor Advisory Committee, and several major comparative-law commentators. Case studies of the Amazon hiring algorithm and the xAI constitutional challenge to Colorado SB 24-205 supplement the doctrinal analysis.

3. The United States: A Layered, Decentralized Regime

The American approach to AI in corporate governance rests on four loosely coupled layers, none of which is sufficient on its own.

3.1 Federal soft law

The October 2022 Blueprint for an AI Bill of Rights articulated five principles — safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, and human alternatives. The Blueprint is explicitly non-binding but has become a reference text for corporate compliance manuals and agency guidance.

The NIST AI Risk Management Framework, released in January 2023, is a more technical voluntary standard. It organizes governance around four functions: GOVERN (leadership accountability, risk tolerance, oversight structures), MAP (system context, stakeholders, intended uses), MEASURE (bias, robustness, security, explainability), and MANAGE (ongoing monitoring and incident response). The AI RMF has been incorporated by reference into procurement clauses, into the now-stayed Colorado AI Act as a safe-harbor benchmark, and into the rulemakings of several state attorneys general.

3.2 Federal sectoral regulation

In the absence of a horizontal AI statute, sectoral regulators have filled the gap. The Securities and Exchange Commission has been the most active. In 2024 and 2025 the agency brought four enforcement actions against registrants for misrepresenting AI capabilities (so-called AI-washing), and AI featured prominently on its 2025 examination priorities. On December 4, 2025, the SEC Investor Advisory Committee voted to recommend that the Commission issue guidance requiring issuers to adopt and disclose a definition of AI, disclose board oversight mechanisms for AI deployment, and report separately on the material effects of AI on internal operations and consumer-facing products. The recommendations are not yet rules, but they have already shaped 2026 proxy season disclosures.

3.3 State statutory experimentation

Several states moved to enact comprehensive AI laws. Colorado Senate Bill 24-205, signed in May 2024, imposed a duty of reasonable care on developers and deployers of high-risk AI used in consequential decisions about employment, housing, credit, insurance, healthcare, education, and legal services. Compliance required impact assessments, deployer risk-management programs, consumer notice, a right to human review, and reporting of discovered algorithmic discrimination. Texas and California enacted parallel statutes. New York City and Illinois moved on AI in employment decisions.

The Colorado experiment encountered three obstacles. First, repeated postponement of the effective date — from February to June 2026 — as definitions proved hard to operationalize. Second, on April 9, 2026, xAI filed a constitutional challenge arguing among other things that the statute compelled developers to engage in race- and sex-conscious model engineering in violation of the Equal Protection Clause; the Department of Justice intervened on April 24, 2026; and a federal magistrate judge stayed enforcement on April 27, 2026. Third, the Colorado legislature rewrote the law through SB 26-189, eliminating the impact-assessment regime and substituting a narrower framework focused on disclosure, human review, and a developer-deployer liability split keyed to relative fault, effective January 1, 2027.

3.4 Federal preemption push

Executive Order 14365 of December 11, 2025 marked a sharp turn toward federal preemption. The order directs federal agencies to identify state AI laws inconsistent with national policy, authorizes the Attorney General to coordinate litigation against such laws through an AI Litigation Task Force, conditions certain federal grants on state alignment, tasks the FTC with issuing a policy statement on preemption of state laws requiring alteration of AI outputs, and asks the FCC to consider a federal reporting standard. The White House National Policy Framework for AI of March 20, 2026 sets out six priorities, including child safety online, intellectual-property protection, prevention of AI-driven censorship, innovation, and workforce readiness.

3.5 Common-law fiduciary backstop

U.S. directors operate under a Delaware-law duty of oversight under the Caremark and Marchand line of cases. A director who knowingly disregards a mission-critical risk can be liable for breach of the duty of care. The May 11, 2026 Southern District of New York decision in the AI-governance oversight matter reinforces that boards cannot delegate substantive responsibility for AI outputs to the algorithm itself. This common-law principle has no direct analogue in many civil-law jurisdictions but functions as an important backstop where statutes are absent or contested.

4. The European Union: A Horizontal, Risk-Based Regime

The European approach is the mirror image of the American one. Where the U.S. has fragmented soft law and contested state statutes, the EU has a single binding regulation that classifies AI by risk and assigns graduated obligations across the value chain.

4.1 The AI Act

Regulation (EU) 2024/1689 of June 13, 2024 — the AI Act — entered into force on August 1, 2024. The Act adopts a four-tier risk classification. Unacceptable-risk practices (social scoring by public authorities, manipulative subliminal techniques, real-time remote biometric identification in public spaces with narrow exceptions) are prohibited. High-risk systems, listed

in Annex III, are subject to extensive obligations including risk-management systems, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, cybersecurity, and post-market monitoring. Limited-risk systems trigger transparency obligations (such as informing users that they are interacting with an AI). Minimal-risk systems are largely unregulated.

Annex III directly implicates corporate governance. It covers AI systems used in recruitment, performance management and termination decisions, credit scoring, insurance underwriting, access to essential services, and several other corporate contexts. Providers, deployers, importers, and distributors each carry distinct obligations along the value chain.

4.2 GDPR Article 22

The General Data Protection Regulation supplies the data-protection layer. Article 22 grants individuals the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects, subject to limited exceptions for contractual necessity, statutory authorization, or explicit consent. Even where exceptions apply, safeguards must protect the data subject's rights and freedoms, including a right to human intervention, to express a viewpoint, and to contest the decision. Article 22 has been the principal European tool for challenging fully automated corporate decisions since long before the AI Act was conceived.

4.3 The Digital Omnibus and the 2027 delay

On November 19, 2025, the European Commission published the Digital Omnibus on AI, a simplification package designed to reduce administrative burden and clarify the interaction between the AI Act and sectoral legislation. On May 7, 2026, the Council of the EU and the European Parliament reached a provisional agreement. Under the agreement, high-risk obligations for standalone Annex III systems are deferred from August 2, 2026 to December 2, 2027, and obligations for high-risk AI embedded in regulated products are deferred until August 2, 2028. Watermarking obligations under Article 50(2) are postponed to December 2, 2026. General-purpose AI rules effective in August 2025, prohibitions effective in February 2025, and other transparency obligations are unchanged.

The delay reflects the practical difficulty of preparing harmonized standards and competent-authority designations in time. The core architecture of the AI Act — risk classification, provider and deployer obligations, and the role of the AI Office — survives the simplification package.

5. Uzbekistan: A State-Led Emerging Framework

Uzbekistan's AI legal architecture rests on three pillars.

The first is Presidential Resolution PP-358 of October 14, 2024, which approved the Strategy for the Development of Artificial Intelligence Technologies until 2030. The Strategy sets quantitative targets: AI-based revenue of 1.5 billion U.S. dollars by 2030, ten AI research laboratories, AI-powered delivery of at least ten percent of public services on the Unified Portal, and a place in the top fifty of the Government AI Readiness Index. It proceeds in three phases — foundational infrastructure through 2025, scaled deployment from 2026 through 2028, and full commercialization from 2028 through 2030.

The second is Cabinet of Ministers Resolution No. 425 of 2025, which identifies priority AI projects for 2025 and 2026 and assigns sectoral implementation responsibilities. The Ministry of

Digital Technologies and the Center for the Development of AI and the Digital Economy coordinate cross-sector implementation.

The third is the law On the Regulation of Relations Arising from the Use of Artificial Intelligence, adopted at first reading by the Legislative Chamber of the Oliy Majlis in April 2025 and approved by the Senate at its eleventh plenary session on November 1, 2025. The law introduces mandatory labelling of AI-generated content, protections against irresponsible AI use, and a general framework for assigning responsibility for AI-related harm.

Three structural gaps remain. First, the principles of fairness, transparency, and human oversight set out in the Strategy have not yet been translated into auditable corporate-governance requirements such as standardized documentation, explainability protocols, or evaluation benchmarks. Second, the November 2025 law focuses on consumer-facing harms and content labelling and does not yet address the use of AI in board-level decision-making, executive compensation, or internal control. Third, there is no securities-style disclosure regime that would oblige listed joint-stock companies to inform shareholders about material AI deployments or board oversight mechanisms.

6. Comparative Analysis

The three regimes can be compared along eight dimensions, summarized in the following table.

Dimension	United States	European Union	Uzbekistan
Regulatory model	Layered and decentralized; sectoral and state experimentation	Horizontal risk-based regulation in a single binding act	State-led strategic planning transitioning to binding rules
Core instruments	Blueprint for an AI Bill of Rights (2022); NIST AI RMF (2023); Executive Order 14365 (2025); state laws	AI Act (Regulation 2024/1689); GDPR Article 22; Digital Omnibus on AI (2026)	Presidential Resolution PP-358 (2024); Cabinet Resolution No. 425 (2025); AI Law (Senate, Nov. 2025)
Legal force	Mostly voluntary at federal level; binding state law often stayed by litigation	Directly binding regulation across all Member States	Mix of binding presidential and cabinet acts plus aspirational principles
Risk classification	No federal classification; some state laws define high-risk by sector	Four-tier system: prohibited, high-risk, limited-risk, minimal-risk	Not yet codified; ethical principles only

Dimension	United States	European Union	Uzbekistan
Corporate governance focus	Securities disclosure and director fiduciary duty under Caremark and Marchand	Risk management, human oversight, transparency, record-keeping for high-risk uses	Not yet addressed; focused on data protection and content labelling
Enforcement actor	SEC, FTC, state attorneys general, federal courts	National competent authorities, AI Office, European Data Protection Board	Ministry of Digital Technologies; Center for the Development of AI and the Digital Economy
Liability allocation	Developer-deployer split based on relative fault (Colorado SB 26-189 model)	Layered duties on providers, deployers, importers, distributors	Not yet defined for AI-specific harms
Implementation status (mid-2026)	Federal preemption push; state laws under constitutional challenge	GPAI rules in force; high-risk obligations deferred to Dec. 2, 2027	Foundational phase of 2024–2030 Strategy; secondary acts under development

Two cross-cutting observations follow. First, although the U.S. and EU regimes differ sharply in legal form (voluntary or sectoral versus horizontal and binding), they converge on several substantive priorities: documenting AI systems, providing human oversight of consequential decisions, allocating liability among actors in the value chain, and disclosing material AI use to investors or consumers. Second, both regimes have encountered the same implementation difficulty — preparing harmonized standards, designating competent authorities, and operationalizing the concept of high-risk before deadlines expire — which is the principal reason for the EU's 2026 delay and the stay of Colorado's statute. A jurisdiction that begins its rulemaking now can avoid these pitfalls by sequencing requirements carefully.

7. General Recommendations for Uzbekistan

Six recommendations follow from the comparative picture. They are designed to be compatible with Uzbekistan's existing institutional architecture and with the 2030 Strategy's ambitions, and to draw on both the U.S. and EU experiences without reproducing the dysfunctions of either.

Recommendation 1. Adopt a closed, risk-based classification of AI uses.

The EU Annex III approach — a closed and amendable list of high-risk use cases — provides more legal certainty than the open-ended formulations that produced definitional disputes under Colorado SB 24-205. Uzbek implementing regulations should classify AI uses

into four tiers (prohibited, high-risk, limited-risk, and minimal-risk), with high-risk explicitly defined to cover employment, credit, insurance, healthcare, education, and law-enforcement applications. The Cabinet of Ministers should retain authority to amend the list as technology evolves.

Recommendation 2. Issue a voluntary national AI risk-management framework.

The Ministry of Digital Technologies, in coordination with the Center for the Development of AI and the Digital Economy, should publish a national AI risk-management framework that mirrors the four functions of the NIST AI RMF (Govern, Map, Measure, Manage). The framework should be initially voluntary and serve as a rebuttable presumption of compliance with the duty of care once binding rules apply to high-risk uses. This sequencing — voluntary standard first, binding rule second — has worked in the U.S. and aligns with the European AI Pact.

Recommendation 3. Introduce a corporate disclosure regime for material AI deployments.

The Capital Markets Development Agency should amend listing rules to require listed joint-stock companies to disclose (i) their working definition of AI, (ii) the board or board-committee mechanism that supervises AI deployment, and (iii) any material AI-related incidents. The disclosure threshold should be materiality, modeled on the SEC Investor Advisory Committee recommendations of December 2025. Disclosure-based regulation is the lowest-cost lever available and creates a market for governance quality.

Recommendation 4. Anchor responsibility at the board level.

The Law on Joint-Stock Companies and Protection of Shareholders' Rights should be amended to clarify that the management board's duty of care extends to the oversight of material AI systems used in corporate decision-making, and that delegation to a vendor or to the algorithm itself does not discharge that duty. This is the civil-law counterpart of the Caremark and Marchand line in the United States.

Recommendation 5. Allocate liability between developer and deployer by relative fault.

Colorado's rewritten SB 26-189 settles on a liability rule that should travel well: a developer is liable when its high-risk AI is used as documented, marketed, and contracted for and still produces discrimination; a deployer is liable when it uses the system outside those parameters. Indemnification clauses that try to shift a party's own liability onto the other should be void as against public policy. This rule respects the relative information advantages of each actor and avoids chilling deployment by small Uzbek firms.

Recommendation 6. Build institutional capacity and international alignment.

Within the existing Coordination Commission for Digital Uzbekistan 2030, an AI Enforcement and Guidance Unit should be empowered to issue interpretative guidance, coordinate with sectoral regulators (banking, capital markets, competition, data protection), and publish an annual report on AI-related corporate-governance incidents. The Unit should engage with the OECD.AI Policy Observatory, the EU AI Office, and the U.S. NIST to ensure that Uzbek standards remain interoperable with the regimes governing the country's principal trading partners.

8. Conclusion

The comparative picture demonstrates that no single jurisdiction has solved the problem of regulating AI in corporate governance. The United States offers an instructive lesson in the costs

of fragmentation: voluntary federal standards have generated useful technical vocabulary, but state statutory experiments have been hampered by definitional disputes, constitutional challenge, and federal preemption pressure. The European Union offers an equally instructive lesson in the difficulty of implementing a horizontal regime: the AI Act is comprehensive, but its high-risk obligations have been deferred to December 2027 because the technical standards and competent-authority designations needed to operationalize them are not yet ready.

Uzbekistan, in contrast, can choose its sequence deliberately. Its strategic framework is in place; its first AI law has passed the Senate; the next steps are to add risk classification, a voluntary risk-management framework, a corporate disclosure regime, board-level oversight duties, a developer-deployer liability split, and the institutional capacity to enforce them. Each of those steps is already drafted in some form in either the American or the European toolkit. Implementing them now, while the architecture is still under construction, will be substantially less costly than retrofitting later, and will make the 2030 Government AI Readiness Index target a regulatory accomplishment as well as a technological one.

References

1. Presidential Resolution of the Republic of Uzbekistan No. PP-358 of October 14, 2024, On the Approval of the Strategy for the Development of Artificial Intelligence Technologies until 2030, https://lex.uz/docs/7159258.

2. Cabinet of Ministers of the Republic of Uzbekistan, Resolution No. 425 of 2025, Priority AI Projects for 2025–2026.

3. Law of the Republic of Uzbekistan, On the Regulation of Relations Arising from the Use of Artificial Intelligence (approved by the Senate of the Oliy Majlis at its 11th plenary session, November 1, 2025).

4. Regulation (EU) 2024/1689 of the European Parliament and of the Council of June 13, 2024, laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), O.J. L, 2024/1689.

5. Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (General Data Protection Regulation), Article 22.

6. European Commission, Proposal for a Regulation on the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM(2025) final, November 19, 2025.

7. Council of the EU and European Parliament, Provisional Agreement on the Digital Omnibus on AI (May 7, 2026), Press Release available at https://www.consilium.europa.eu.

8. European Commission, AI Act — Implementation Timeline, Shaping Europe's Digital Future, https://digital-strategy.ec.europa.eu.

9. White House, Office of Science and Technology Policy, Blueprint for an AI Bill of Rights (October 2022), https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/.

10. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (January 26, 2023).

11. Executive Order 14365, Ensuring a National Policy Framework for Artificial Intelligence (December 11, 2025).

12. White House, National Policy Framework for Artificial Intelligence (March 20, 2026).

13. Colorado Senate Bill 24-205, Consumer Protections for Artificial Intelligence (signed May 17, 2024).

14. Colorado Senate Bill 26-189, An Act Concerning Accountability for Automated Decision-Making Technology (2026), effective January 1, 2027.

15. xAI Corp. v. Weiser, No. 1:26-cv-XXXXX (D. Colo. filed April 9, 2026); U.S. Department of Justice Complaint in Intervention (April 24, 2026); Order Staying Enforcement (April 27, 2026).

16. U.S. Securities and Exchange Commission, Investor Advisory Committee, Recommendation Regarding Disclosure of Artificial Intelligence's Impact on Operations (December 4, 2025).

17. In re Caremark Int'l Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996); Marchand v. Barnhill, 212 A.3d 805 (Del. 2019).

18. OECD.AI Policy Observatory, The Strategy for the Development of Artificial Intelligence Technologies until 2030 — Uzbekistan (last updated 2025).

19. Ernst and Young, Study on the Relevance and Impact of Artificial Intelligence for Company Law and Corporate Governance — Final Report (2021), prepared for the European Commission.

20. BBC News, Amazon scrapped "sexist AI" tool (October 10, 2018), https://www.bbc.com/news/technology-45809919.