eISSN: 2229-3213 pISSN: 2229-3205
The Journal of Applied Science and Social Science
Volume 16,Issue 03 March, 2026

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 transforming how companies make decisions, run internal controls, and handle disclosure throughout every leading economy. Even so, the legal regimes that determine how firms use AI within their governance structures vary widely from one jurisdiction to another. This article presents a brief comparative survey of three distinct models. The United States has developed a fragmented, multi-tiered system resting on voluntary federal benchmarks, sector-specific securities oversight, and competing state statutes, more recently layered with an executive-branch effort to assert federal preemption. The European Union has chosen a horizontal, risk-graded approach in its 2024 AI Act, reinforced by the General Data Protection Regulation and the Digital Omnibus simplification package of November 2025. Uzbekistan has advanced quickly from strategic planning under Presidential Resolution PP-358 of October 2024 to a wide-ranging AI statute cleared by the Senate in November 2025, though several corporate-governance shortcomings persist. After charting each system, the article draws out six broad proposals for reform in Uzbekistan, centered on risk classification, board-level supervision, 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

Within just three years, artificial intelligence has shifted from an experimental aid for decisions to a central operational component of corporate governance. Boards today depend on AI to filter hiring pipelines, score credit requests, uncover fraud, track compliance, prepare disclosures, and shape strategic acquisitions. The legal issue is no longer whether the corporate use of AI should be regulated, but how to do so without stifling innovation or transferring risk onto markets that are unprepared for it.

Three jurisdictions illustrate the main regulatory paths that any nation, Uzbekistan included, has to weigh. The United States embodies a layered, decentralized approach: voluntary federal standards paired with sectoral oversight (notably in securities), state-level legislative trials, and a recent federal move toward preemption. The European Union exemplifies a horizontal, risk-based approach built around the 2024 AI Act and bolstered by the General Data Protection Regulation. Uzbekistan reflects a state-driven model in which strategic planning has thus far run ahead of detailed legal rules.

This article charts the three systems, sets them alongside one another, and advances six broad proposals for Uzbek reform. The aim is comparative rather than prescriptive: Uzbekistan

does not have to pick between the American and European blueprints, but can take from each the components that suit its institutional capacity and economic goals.

2. Methods and Materials

The study applies a doctrinal and comparative legal approach. Primary sources 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, version 1.0 of the NIST AI Risk Management Framework from 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, Uzbek Presidential Resolution PP-358 of October 14, 2024, Cabinet of Ministers Resolution No. 425 of 2025, and the Uzbek AI Law passed by the Senate of the Oliy Majlis at its eleventh plenary session on November 1, 2025. Secondary sources comprise reports from the Council of the European Union, the European Parliament, the U.S. Securities and Exchange Commission Investor Advisory Committee, and a number of leading comparative-law scholars. The doctrinal analysis is supplemented by case studies of Amazon's hiring algorithm and xAI's constitutional challenge to Colorado SB 24-205.

3. The United States: A Layered, Decentralized Regime

The U.S. treatment of AI in corporate governance rests on four loosely connected layers, no one of which suffices by itself.

3.1 Federal soft law

The Blueprint for an AI Bill of Rights, released in October 2022, set out five principles: systems that are safe and effective, safeguards against algorithmic discrimination, data privacy, notice and explanation, and human alternatives. Although expressly non-binding, the Blueprint has become a touchstone for corporate compliance manuals and agency guidance.

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

3.2 Federal sectoral regulation

Without a horizontal AI statute, sectoral regulators have stepped into the breach. The Securities and Exchange Commission has been the busiest of them. Across 2024 and 2025 the agency pursued four enforcement actions against registrants for overstating AI capabilities — so-called AI-washing — and AI ranked high among its 2025 examination priorities. On December 4, 2025, the SEC Investor Advisory Committee voted to advise the Commission to issue guidance requiring issuers to adopt and disclose a definition of AI, reveal board oversight arrangements for AI deployment, and report separately on the material effects of AI on internal operations and on consumer-facing products. These recommendations are not yet rules, but they have already influenced disclosures in the 2026 proxy season.

3.3 State statutory experimentation

A number of states moved to enact comprehensive AI laws. Colorado Senate Bill 24-205, signed in May 2024, placed a duty of reasonable care on developers and deployers of high-risk AI used in consequential decisions concerning employment, housing, credit, insurance, healthcare, education, and legal services. Meeting that duty required impact assessments, deployer risk-management programs, consumer notice, a right to human review, and reporting of any algorithmic discrimination uncovered. Texas and California passed comparable laws, while New York City and Illinois acted on AI in employment decisions.

The Colorado initiative ran into three difficulties. The first was repeated delay of the effective date — slipping from February to June 2026 — as the definitions proved difficult to put into practice. The second came on April 9, 2026, when xAI brought a constitutional challenge contending, among other points, that the statute forced developers into race- and sex-conscious model engineering in breach 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. The third was the Colorado legislature's overhaul of the law via SB 26-189, which scrapped the impact-assessment scheme and replaced it with a narrower structure built around disclosure, human review, and a developer–deployer liability division tied to relative fault, taking effect on January 1, 2027.

3.4 Federal preemption push

Executive Order 14365 of December 11, 2025 signaled a decisive pivot toward federal preemption. It instructs federal agencies to flag state AI laws at odds with national policy, empowers the Attorney General to coordinate litigation against such laws through an AI Litigation Task Force, ties certain federal grants to state alignment, charges the FTC with issuing a policy statement on preempting state laws that demand changes to AI outputs, and invites the FCC to weigh a federal reporting standard. The White House National Policy Framework for AI of March 20, 2026 lays out six priorities, among them online child safety, intellectual-property protection, guarding against AI-driven censorship, innovation, and workforce readiness.

3.5 Common-law fiduciary backstop

U.S. directors are subject to a Delaware-law duty of oversight under the Caremark and Marchand line of authority. A director who deliberately ignores a mission-critical risk may be held liable for breaching the duty of care. The Southern District of New York's decision of May 11, 2026 in the AI-governance oversight case underscores that boards may not hand off substantive responsibility for AI outputs to the algorithm itself. While this common-law doctrine lacks a direct equivalent in many civil-law systems, it serves as a valuable safety net where statutes are missing or disputed.

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

The European model is the inverse of the American one. Whereas the U.S. relies on fragmented soft law and contested state statutes, the EU has a single binding regulation that sorts AI by risk and assigns escalating obligations across the value chain.

4.1 The AI Act

Regulation (EU) 2024/1689 of June 13, 2024 — the AI Act — took effect on August 1, 2024. The Act sets up a four-tier risk taxonomy. Unacceptable-risk practices (social scoring by public authorities, manipulative subliminal methods, and real-time remote biometric identification in public spaces, subject to narrow exceptions) are banned outright. High-risk systems, enumerated in Annex III, face extensive requirements covering risk-management systems, data governance, technical documentation, record-keeping, transparency, human oversight, accuracy, robustness, cybersecurity, and post-market monitoring. Limited-risk systems carry transparency duties — such as telling users they are dealing with an AI — while minimal-risk systems are largely left alone.

Annex III bears directly on corporate governance. It encompasses AI used in recruitment, performance review and termination decisions, credit scoring, insurance underwriting, access to essential services, and various other corporate settings. Providers, deployers, importers, and distributors each bear separate obligations along the value chain.

4.2 GDPR Article 22

The General Data Protection Regulation furnishes the data-protection layer. Article 22 confers on individuals the right not to be subjected to a decision based solely on automated processing, profiling included, that yields legal or similarly significant effects, save for limited exceptions tied to contractual necessity, statutory authorization, or explicit consent. Even where an exception applies, safeguards must protect the data subject's rights and freedoms, including a right to human intervention, to voice a viewpoint, and to contest the outcome. Long before the AI Act was envisioned, Article 22 served as Europe's chief instrument for challenging wholly automated corporate decisions.

4.3 The Digital Omnibus and the 2027 delay

On November 19, 2025, the European Commission released the Digital Omnibus on AI, a simplification package meant to ease administrative burden and clarify how the AI Act interacts with sectoral law. On May 7, 2026, the Council of the EU and the European Parliament struck a provisional agreement. Under it, high-risk obligations for standalone Annex III systems are pushed back from August 2, 2026 to December 2, 2027, while those for high-risk AI embedded in regulated products are delayed to August 2, 2028. Watermarking duties under Article 50(2) are postponed to December 2, 2026. The general-purpose AI rules effective in August 2025, the prohibitions effective in February 2025, and other transparency obligations remain in place.

The postponement reflects how hard it is to ready harmonized standards and designate competent authorities in time. The AI Act's core design — risk classification, provider and deployer obligations, and the AI Office's role — endures through the simplification package.

5. Uzbekistan: A State-Led Emerging Framework

Uzbekistan's legal architecture for AI stands on three pillars.

The first is Presidential Resolution PP-358 of October 14, 2024, which adopted the Strategy for the Development of Artificial Intelligence Technologies until 2030. The Strategy fixes quantitative goals: 1.5 billion U.S. dollars in AI-derived revenue by 2030, ten AI research laboratories, AI-enabled delivery of at least ten percent of public services on the Unified Portal, and a top-fifty position on the Government AI Readiness Index. It unfolds across three phases — foundational infrastructure through 2025, scaled rollout from 2026 to 2028, and full

commercialization from 2028 to 2030.

The second is Cabinet of Ministers Resolution No. 425 of 2025, which singles out priority AI projects for 2025 and 2026 and allocates sectoral implementation duties. The Ministry of Digital Technologies together with the Center for the Development of AI and the Digital Economy coordinates implementation across sectors.

The third is the law On the Regulation of Relations Arising from the Use of Artificial Intelligence, passed 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 brings in mandatory labelling of AI-generated content, safeguards against irresponsible AI use, and a general scheme for assigning responsibility for AI-related harm.

Three structural gaps persist. First, the Strategy's principles of fairness, transparency, and human oversight have not yet been converted into auditable corporate-governance requirements such as standardized documentation, explainability protocols, or evaluation benchmarks. Second, the November 2025 law concentrates on consumer-facing harms and content labelling and does not yet reach the use of AI in board-level decisions, executive pay, or internal control. Third, no securities-style disclosure regime yet requires listed joint-stock companies to brief shareholders on material AI deployments or on board oversight mechanisms.

6. Comparative Analysis

The three regimes can be set against one another along eight dimensions, as summarized in the table below.

Dimension	United States	European Union	Uzbekistan
Regulatory model	Multi-layered and decentralized, driven by sector-specific rules and state-level experiments	A single binding statute organized horizontally around risk	Government-led strategic planning now shifting toward enforceable rules
Core instruments	AI Bill of Rights Blueprint (2022); NIST AI RMF (2023); Executive Order 14365 (2025); various state statutes	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	Largely voluntary federally; binding state measures frequently halted by litigation	A regulation that binds directly throughout all Member States	A combination of binding presidential and cabinet acts alongside aspirational principles

Risk classification	No nationwide scheme; certain states designate high-risk categories by sector	Four tiers: prohibited, high-risk, limited-risk, and minimal-risk	Not yet codified; only ethical principles exist
Corporate governance focus	Securities disclosure plus director fiduciary duties under Caremark and Marchand	Risk management, human oversight, transparency, and record-keeping for high-risk applications	Not yet covered; attention is on data protection and content labelling
Enforcement actor	SEC, FTC, state attorneys general, and federal courts	National competent authorities, the AI Office, and the European Data Protection Board	Ministry of Digital Technologies; Center for the Development of AI and the Digital Economy
Liability allocation	Fault-based division between developer and deployer (the Colorado SB 26-189 approach)	Tiered duties spread across providers, deployers, importers, and distributors	Not yet specified for AI-related harms
Implementation status (mid-2026)	Federal preemption drive underway; state statutes facing constitutional litigation	GPAI rules active; high-risk duties pushed back to Dec. 2, 2027	Foundational stage of the 2024–2030 Strategy; secondary legislation in progress

Two cross-cutting points emerge. First, although the U.S. and EU regimes differ markedly in legal form — voluntary or sectoral as against horizontal and binding — they align on several substantive priorities: documenting AI systems, ensuring human oversight of consequential decisions, distributing liability among value-chain actors, and disclosing material AI use to investors or consumers. Second, both regimes have run into the same implementation hurdle — readying harmonized standards, designating competent authorities, and giving operational meaning to the high-risk concept before deadlines lapse — which is the main reason behind the EU's 2026 delay and the stay of Colorado's statute. A country that starts its rulemaking now can sidestep these traps by sequencing requirements with care.

7. General Recommendations for Uzbekistan

Six recommendations follow from the comparative picture. They are crafted to fit Uzbekistan's existing institutional architecture and the ambitions of the 2030 Strategy, and to borrow from both the U.S. and EU experiences without importing the dysfunctions of either.

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

The EU's Annex III method — a closed but amendable roster of high-risk use cases — offers greater legal certainty than the open-ended phrasing that triggered definitional disputes

under Colorado SB 24-205. Uzbek implementing regulations should slot AI uses into four tiers (prohibited, high-risk, limited-risk, and minimal-risk), with high-risk expressly defined to capture employment, credit, insurance, healthcare, education, and law-enforcement applications. The Cabinet of Ministers should keep the power to revise the list as the technology develops.

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

The Ministry of Digital Technologies, working with the Center for the Development of AI and the Digital Economy, should publish a national AI risk-management framework patterned on the four functions of the NIST AI RMF (Govern, Map, Measure, Manage). At the outset the framework should be voluntary and operate as a rebuttable presumption of compliance with the duty of care once binding rules attach to high-risk uses. This ordering — a voluntary standard first, a binding rule second — has proven workable in the U.S. and is consistent with the European AI Pact.

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

The Capital Markets Development Agency should revise listing rules to require listed joint-stock companies to disclose (i) their working definition of AI, (ii) the board or board-committee mechanism overseeing AI deployment, and (iii) any material AI-related incidents. The disclosure trigger should be materiality, modeled on the SEC Investor Advisory Committee's December 2025 recommendations. Disclosure-based regulation is the least costly lever available and fosters 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 make clear that the management board's duty of care reaches the oversight of material AI systems used in corporate decision-making, and that delegating to a vendor or to the algorithm itself does not relieve the board of that duty. This is the civil-law analogue of the Caremark and Marchand line in the United States.

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

Colorado's revised SB 26-189 lands on a liability rule that ought to transfer well: a developer is liable when its high-risk AI is used as documented, marketed, and contracted for yet still produces discrimination; a deployer is liable when it operates the system outside those bounds. Indemnification clauses that attempt to push one party's own liability onto the other should be unenforceable as contrary to public policy. The rule honors each actor's relative informational advantages and avoids deterring 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 authorized to issue interpretative guidance, coordinate with sectoral regulators (banking, capital markets, competition, data protection), and release 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 so that Uzbek

standards stay interoperable with the regimes of the country's main trading partners.

8. Conclusion

The comparative picture shows that no single jurisdiction has cracked the problem of regulating AI in corporate governance. The United States provides a cautionary lesson about the price of fragmentation: voluntary federal standards have produced a useful technical vocabulary, yet state legislative experiments have been hampered by definitional disputes, constitutional litigation, and pressure from federal preemption. The European Union offers an equally instructive lesson about the difficulty of operating 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 implement them are not yet in place.

Uzbekistan, by contrast, can choose its sequence deliberately. Its strategic framework is established and its first AI law has cleared the Senate; the next moves 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 already exists in some shape in either the American or the European toolkit. Putting them in place now, while the architecture is still being built, will be far cheaper than retrofitting later, and will turn the 2030 Government AI Readiness Index target into a regulatory achievement as much 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-4580