

Bernaziuk Inna,
Professor, Department of Law,
European University (Ukraine),
Doctor of Laws,
Honoured Lawyer of Ukraine
ORCID: 0000-0002-8460-2687;
e-mail: innabernaziuk@gmail.com

**ARTIFICIAL INTELLIGENCE IN CORPORATE GOVERNANCE:
PERMISSIBLE AUTONOMY, HUMAN OVERSIGHT AND
CONSTITUTIONAL LIMITS OF PUBLIC SUPERVISION**

Abstract. The article examines the legal limits of using artificial intelligence (AI) in corporate governance and the relationship between corporate autonomy and public supervision. It employs formal legal, comparative, systemic and functional methods and analyses legislation, soft-law instruments, regulatory documents and the Federal Court of Australia's judgment in ASIC v Bekier. The central issue for corporate law is not the legal personality of AI but the limits within which functions may be entrusted to AI in the preparation, adoption and implementation of corporate decisions. The statutory competence of corporate bodies is identified as the primary legal limit: particular functions may be entrusted to AI, but neither corporate competence itself nor responsibility for its exercise. The article argues that the statutory standard of care, skill and diligence of corporate officers encompasses the proper organisation of AI use. The limits of public supervision are examined through the constitutional requirements of legality, legitimate aim and proportionality (Articles 8, 13, 19, 42 and 92 of the Constitution of Ukraine). A criterion distinguishing the assessment of the adequacy of AI governance systems and decision-making procedures from the assessment of the substance of business decisions is proposed to delineate public supervision and corporate discretion. The article also examines the potential of AI to reduce corruption risks in corporate governance, particularly in companies with state ownership, and the conditions for realising that potential. For Ukraine, the article proposes a three-level regulatory model and a model of four regimes for corporate AI use based on system autonomy, decision materiality, external risk and controllability, taking into account the amendments to Regulation (EU) 2024/1689 introduced by Regulation (EU) 2026/1744.

Keywords: artificial intelligence, corporate governance, corporate law, corporate decision, human oversight, corporate discretion, risk management, public supervision, freedom of enterprise, corruption prevention, state ownership.

Statement of the Problem

Artificial intelligence (AI) is increasingly used to analyse corporate information, assess risks, forecast the consequences of decisions, monitor compliance with established requirements, draft management instruments and carry out individual operations. Ukrainian scholarship identifies a need to delineate the limits of AI use in corporate governance and the growing importance of internal corporate regulation [2, pp. 112–118; 9, pp. 98–112; 10, pp. 76–83]. In particular, the prospects for legal regulation are associated not with recognising AI as a legal person, but with creating mechanisms for control, accountability and safety [10, pp. 80–82].

International scholarship considers AI not merely an aid to executives but also an element of the work of boards of directors or supervisory boards, internal control, risk management and information exchange among corporate bodies [3, pp. 8–25; 4, pp. 43–55; 7, pp. 15–21; 11, pp. 631–636]. AI systems can reduce information asymmetry, but they also create new risks of managers' dependence on automated analysis and may weaken the relevant corporate body's capacity to exercise oversight [3, pp. 25–30; 4, pp. 52–58]. Researchers trace a shift towards agentic AI systems capable of independently carrying out certain operations within established limits [3; 21, pp. 1–3]. Legal regulation should enable extensive AI use while preserving clarity as to corporate competence, responsibility and effective control.

This article aims to develop a legal model that proceeds from the permissibility of active AI use and strengthens legal safeguards only in proportion to risk.

State of the Research

In examining the legal nature of AI, Ukrainian legal scholarship demonstrates that technological autonomy is not equivalent to a legally independent will, while a legal entity exercises its legal personality through its corporate bodies [9, pp. 104–110; 10, pp. 79–82].

Regarding the degree of AI involvement in corporate governance, Hilb proposes a progression from auxiliary to autonomous governance [6, pp. 855–861]. Hickman and Petrin examine different models of human oversight [18, pp. 610–618]. Möslin emphasises a qualitative distinction between AI and earlier forms of digitalisation: AI not only accelerates access to information but also directly influences how decisions are formed [11, p. 631].

In the context of responsibility and oversight, Petrin substantiates the relationship between a corporation's external liability for harm and the internal duties of its managers [7, pp. 17–21]. The further development of agentic systems may increase the importance of corporate liability for failures in organisational arrangements, rather than solely the personal liability of a particular individual [21, pp. 1–3, 24–27].

Empirical studies of major corporations show that the existence of policies, committees and declarations does not in itself establish adequate governance. Independent review, assessment of effectiveness, inventories of material systems and incident reporting remain problematic [8, sections 5–6; 13, pp. 31–38].

The progressive examination of the legal limits of AI can also be traced through the author's previous publications: in banking, the protection of customers' rights and a risk-based regulatory model were considered [37]; in insurance, the limits of algorithmic risk assessment and claims decisions [38]; and in lobbying, the constitutional principles of transparency and prevention of improper influence [39]. Those studies primarily concerned the external legal consequences of AI use. The present article focuses on the internal allocation of corporate competence and responsibility and on the limits of public supervision.

Nevertheless, insufficient attention has been paid to the corporate-law boundary governing the permissible assignment of particular functions of corporate bodies to AI and its relationship with the limits of public supervision. This forms the subject of the present study.

The article's scientific contribution lies in identifying the limits of AI autonomy in corporate governance by reference to the statutory allocation of competence among corporate bodies, the standard of proper conduct required of corporate officers as elaborated in the case law of the Grand Chamber of the Supreme Court, and

constitutional guarantees of freedom of enterprise. It proposes a criterion for distinguishing procedural oversight from the assessment of the substance of a business decision, designed to ensure proportionality in public supervision, together with a three-tier regulatory model and four regimes of corporate AI use that do not displace statutory risk classifications.

1. Limits of Permissible AI Autonomy in Corporate Governance

The debate over AI's independent legal personality has limited practical significance for corporate law. It does not alter the fundamental legal structure: a legal entity exercises its legal capacity through bodies established by law and its constituent documents.

This structure is embodied in Ukrainian corporate legislation. Article 39 of the Law of Ukraine 'On Joint Stock Companies' sets out the exclusive competence of the general meeting and prohibits transferring the relevant powers to other corporate bodies [24, Article 39(2)–(3)]. Depending on the company's governance structure, the Law defines the powers of the board of directors or supervisory board [24, Articles 4, 63 and 71].

A comparable framework applies to limited and additional liability companies. Matters assigned by law to the general meeting cannot be assigned to other bodies unless otherwise provided by law [34, Article 30(3)]; powers of the general meeting may be delegated to the supervisory board except for matters within the meeting's exclusive competence [34, Article 38(4)]; and the executive body manages current operations except for matters exclusively reserved to the general meeting or supervisory board [34, Article 39(2)].

An additional safeguard is the prohibition on a member of a collegial executive body of a limited liability company transferring their vote to another person [34, Article 39(11)]. This precludes substituting an AI system's decision for the personal expression of a member's vote, without preventing technical automation of voting procedures within statutory limits. A legal entity continues to exercise its civil rights and obligations through its bodies [36, Article 92(1)]; accordingly, an agentic system's actions must remain within the tasks and powers defined by the competent corporate body or authorised individual.

Thus, the first legal limit on AI autonomy already follows from existing corporate law: AI use cannot substitute for the exercise of competence that the law assigns to the relevant corporate body. AI may contribute to assembling the information base, preparing alternatives and implementing a decision, but does not thereby become the holder of competence vested by law in that body.

This does not mean, however, that AI must be confined to purely technical assistance. It may analyse information, assess risks, predict outcomes, prepare decision options, monitor implementation and perform particular acts within defined powers, rules and conditions for human intervention, provided that this is consistent with the law and the legal entity's internal instruments. Greater system efficiency does not justify extending its role beyond those limits. Legal regulation should therefore address the conditions under which AI may perform individual functions while preserving corporate competence and responsibility for its exercise.

Regulation (EU) 2024/1689 is not part of Ukrainian domestic law, but it provides a benchmark for European integration. Its requirements may apply directly to Ukrainian entities under the conditions laid down in Article 2, particularly where AI systems are placed on the market or put into service in the EU or their outputs are used in the EU [15, Article 2].

Permissible AI autonomy is proposed to be determined by four interrelated criteria, whose content and application are examined in Section 5. This approach is consistent with the risk-based logic of Regulation (EU) 2024/1689 [15, Articles 6, 9 and 14; Annex III], the OECD Recommendation on AI [17, sections 1.1–1.5], the US National Institute of Standards and Technology's AI Risk Management Framework (NIST AI RMF) [16, pp. 20–34], and Ukrainian regulatory approaches [23, pp. 10–18; 32, pp. 12–23].

Corporate freedom nevertheless has limits. Annex III to Regulation (EU) 2024/1689 specifically classifies as high-risk certain systems used in employment, worker management and access to self-employment, as well as certain systems assessing the creditworthiness of natural persons [15, Annex III, points 4–5]. The Regulation imposes specific requirements for risk management, documentation, transparency and human oversight for such systems. Following the amendments introduced by

Regulation (EU) 2026/1744, the requirements in Sections 1–3 of Chapter III for systems classified as high-risk under Article 6(2) and Annex III apply from 2 December 2027, subject to transitional provisions [15, Articles 9–15, 111 and 113].

For systems subject to those requirements, Article 14 of the Regulation obliges providers to design appropriate human-oversight measures into high-risk systems. Under Article 26, deployers must assign that oversight to natural persons with the necessary competence, training, authority and support [15, Article 14; Article 26(2)].

Article 4 of Regulation (EU) 2024/1689, as amended by Regulation (EU) 2026/1744, requires providers and deployers to take measures to develop AI literacy among their staff and other persons dealing with these systems on their behalf, taking account of their knowledge, experience, training and the circumstances of use; it does not require a specified level of literacy to be guaranteed for every individual [15, Article 4].

Ukrainian corporate law, in turn, establishes its own standard of conduct for officers. Officers of a joint stock company must act with a reasonable degree of care, skill and diligence, assessed in light of both objectively expected knowledge and the knowledge, skills and experience appropriate to the particular officer [24, Article 89(7)]. Where AI is systematically used to prepare material decisions, understanding its capabilities and limitations becomes part of that standard.

Merely obtaining a person's formal approval of an AI output is insufficient. The authorised person must have the information, competence, time and powers necessary to review, reject or modify that output.

These considerations justify differentiated access for AI to corporate operations: the permitted degree of autonomy may increase within a defined regime as risk decreases and verification and human-intervention mechanisms improve.

2. Proper Organisation of AI Use as an Element of Corporate Duties

AI use changes what proper discharge of duties by members of corporate bodies entails in practice. Legal assessment concerns not only the outcome of a decision but also whether AI use was appropriately organised.

This approach accords with Article 92(3) of the Civil Code of Ukraine, which requires a person acting on behalf of a legal entity to act in its interests, in good faith, reasonably and within their powers. For joint stock companies, these duties are elaborated in

Article 89 of the Law of Ukraine 'On Joint Stock Companies' [36, Article 92(3); 24, Article 89(4)–(7)].

Article 89(5) of that Law requires officers to act in the manner they believe in good faith is most likely to promote the company's successful performance, while Article 89(6) requires independent decision-making [24, Article 89(5)–(6)]. Although Ukrainian legislation does not establish the business judgment rule as a separate legal doctrine, before the enactment of Law No. 2465-IX the Grand Chamber of the Supreme Court articulated a presumption that an officer had properly performed fiduciary duties, including the independence and reasoned basis of decisions. Once the claimant rebuts that presumption on at least one criterion, the defendant must demonstrate that they acted in the company's interests [41, paragraphs 7.17–7.19]. In the AI context, uncritical reproduction of the output of an unverified system may indicate a lack of independent and reasoned judgment, while substantive review of that output may serve as evidence of proper conduct by the officer.

Traditional requirements of good faith, reasonableness, informed judgment and respect for allocated powers take on new practical significance when AI is used. If a corporate body systematically relies on a system whose suitability has not been tested, or lacks information about material systems deployed within the company, a formal assertion of good faith cannot suffice [7, pp. 15–21; 12; 20, pp. 33–42]. For the purposes of this study, an AI system is proposed to be considered material where its use may have significant legal or financial consequences for the company or third parties, including in preparing decisions reserved to corporate bodies, autonomously carrying out significant operations, affecting employees', customers', investors' or creditors' rights, or complying with material regulatory requirements.

Depending on the nature and risk of the system, proper organisation of AI use may entail an internal inventory of material systems; risk classification; designation of a responsible body or officer; sufficient competence among members of management bodies; testing system suitability and input-data quality; recording material circumstances of use; enabling subsequent review; and establishing procedures for responding to deviations and incidents [1; 5, pp. 368–372; 8, sections 5–6; 14, pp. 11–18].

For joint stock companies, the legal basis for this approach includes the supervisory board's authority to approve relevant internal regulations and a risk appetite declaration [24, Article 71(2), points 1 and 14²]. This makes it possible to integrate AI risk management into the existing corporate governance framework without creating parallel bodies or procedures.

At the same time, such a standard must not become a merely formal checklist. Gan, Wilczek-Stronczek and Papasava demonstrate that visible governance structures are developing faster than mechanisms for assessing their actual effectiveness [8, sections 5–6]. The law should evaluate whether internal instruments can genuinely manage risk. The fact of AI use neither releases an officer from liability nor creates a presumption of breach. Uncritical reliance on AI outputs when making a material corporate decision may indicate improper discharge of an officer's duties. Current legislation establishes no general duty to use AI. Nevertheless, the relevance of available, appropriately tested systems to assessing whether a corporate decision was sufficiently informed warrants further research.

A related approach can be found in comparative corporate law. In *Australian Securities and Investments Commission v Bekier (Liability Judgment)* [2026] FCA 196 (5 March 2026), the Federal Court of Australia considered the conditions governing the business judgment rule in section 180(2) of the Corporations Act 2001 (Cth), which, subject to statutory conditions, protects good-faith, informed business decisions [35, paragraphs 407–423]. Section 189 of that Act provides for a presumption of reasonable reliance by a director on information or advice from specified persons, provided the director acts in good faith and makes an independent assessment [35, paragraphs 424–425; 47, section 189]. That presumption does not directly extend to AI outputs, but the requirement of independent judgment may be applied by analogy. Accordingly, merely approving an AI output does not establish that a director has properly discharged their duties.

In the same case, the Court observed that using AI to process board materials is not inherently objectionable, but directors must retain the ability to evaluate the information independently [35, paragraphs 390–396]. In its concluding observations, the Court further stressed that technology may facilitate understanding but cannot

replace human judgment; a director's duty under section 180(1) remains personal [35, paragraph 1956]. These observations concerning AI are obiter dicta and are invoked here as a comparative-law argument; they do not establish independent grounds of liability.

3. Corporate Discretion and the Limits of Public Supervision

AI use in regulated sectors requires a clear distinction between corporate discretion and the competence of public regulators. The constitutional basis for that distinction operates in two directions. Article 42 of the Constitution of Ukraine guarantees the freedom to engage in entrepreneurial activity not prohibited by law, while also requiring the state to protect competition and consumer rights. The principle that ownership entails obligations and must not be used to the detriment of individuals or society further supports the public interest in supervising AI-related risks [40, Article 13(3), Article 42(1), (3) and (4)].

Together with Articles 8, 19 and 92 of the Constitution of Ukraine, these provisions establish three requirements for public intervention: an adequate legal basis, a legitimate aim involving the protection of constitutionally significant interests, and proportionality of the restriction [40, Article 8(1), Article 19(2), Article 92(1)(8) and (2)(1)]. The proposed distinction between assessment of the adequacy of a system and its procedures, on the one hand, and assessment of the substance of a business decision, on the other, gives effect to these requirements: where proper system oversight is capable of achieving the legitimate aim, state intervention should not replace a lawful business choice. This approach accords with the Constitutional Court of Ukraine's position linking freedom of enterprise with effective protection of consumer rights and recognising proportionality as a necessary requirement of the rule of law [44, section 3, subparagraph 3.8; section 4, subparagraph 4.1].

Review of legality should not replace corporate discretion with an assessment of a decision's economic expediency, except where such assessment falls within the powers conferred on the regulator by law. At the same time, banking, financial and investment activities engage the public interest in market stability and the protection of consumers, investors and creditors [25; 26].

Within their statutory powers, public authorities may supervise the correctness of risk classification, designation of responsible persons, effectiveness of human oversight, auditability of material operations, internal controls, protection of third-party rights and appropriate responses to incidents. By contrast, the choice among lawful commercial alternatives should remain within the competence of corporate bodies. In this respect, the judicially recognised presumption of proper performance of fiduciary duties and the proposed criterion serve related, though distinct, functions: protecting properly exercised corporate discretion against unjustified retrospective reassessment.

The priority given to procedural supervision does not preclude review of the substance of a corporate decision for compliance with substantive law and safeguards for third-party rights. Persons whose rights are infringed by a corporate decision made with AI assistance retain the right to judicial protection [40, Article 55(1)], while a business entity retains the right to challenge unlawful supervisory intervention by a public authority [40, Article 55(2)]. Freedom of enterprise does not protect corporate decisions contrary to law.

Ukrainian financial regulation already contains structures suitable for this approach. National Bank of Ukraine (NBU) Regulation No. 64 provides for an organised risk management system and internal instruments defining relevant procedures [27]. NBU Regulation No. 185 establishes corporate governance and internal control requirements for financial companies [28, points 1–2 of the Resolution; points 1–3 of the Regulation]. The NBU's methodological recommendations employ the concept of collective suitability of management bodies [29, point 2], covering the adequacy of their aggregate knowledge, skills and experience.

Of particular significance is the NBU's 2026 Discussion Paper, which expressly links AI use to risk-based management, protection of consumers' rights, data and model management and operational resilience [23, sections V–VIII].

J.-M. Bello y Villarino and S. Bronitt discuss the possibility of automated compliance-monitoring systems under which regulators primarily assess the reliability of internal systems and a company's response to indications of non-compliance [22, pp. 365–367]. This model may improve supervisory effectiveness but must respect proportionality so that it does not become a means of unlimited, continuous state access to corporate data.

4. A Three-Tier Model of AI Regulation in Ukraine

Ukraine's Strategy for the Digital Development of Innovation Activities through 2030 identifies innovation-led development as a direction of public policy [31], while the Ministry of Digital Transformation's White Paper proposes a phased approach to preparing future regulation [32, pp. 4–9, 20–26].

Three regulatory tiers are proposed for the corporate sphere: legislative, sector-specific and internal corporate. They must be distinguished from the four regimes of corporate AI use developed in Section 5.

The first tier is general legislation. It should establish baseline safeguards, principles of liability and requirements for high-risk systems. The principal European reference point is Regulation (EU) 2024/1689 as amended by Regulation (EU) 2026/1744 [15, Articles 6, 9–15 and 26; Annex III]. Its risk-based approach does not, however, permit the most stringent requirements to be mechanically imposed on all corporate uses of AI. As the legal foundations and guarantees of entrepreneurship must be determined by legislation, binding requirements for high-risk systems must have a statutory basis [40, Article 92(1)(8)].

The second tier is sector-specific regulation. Ukrainian legislation on financial services and capital markets establishes particular regimes of public supervision [25; 26], while NBU instruments provide mechanisms for risk management, internal control and corporate governance [27–29]. This permits AI-related requirements to be incorporated into existing risk management systems without creating parallel regulatory structures, within the limits of powers granted to regulators by law [40, Article 19(2)].

AI has particular significance for state-owned enterprises and companies with state participation. The amendments introduced by Law of Ukraine No. 3587-IX of 22 February 2024 strengthened the normative role of supervisory boards, internal control and accountability in the governance of public-sector entities [46]. Automated detection of anomalies in procurement, settlements and transactions, examination of relationships between counterparties and documentation of the grounds for decisions may reduce the risks of conflicts of interest, selective treatment and improper influence over the management of state assets [42]. Such tools should be integrated into anti-corruption programmes of legal entities covered by Article 62 of the Law of Ukraine

'On Prevention of Corruption' [43]. As argued in the author's earlier research, algorithmic identification of corruption risk must be distinguished from a legal finding of wrongdoing [45]. In corporate governance, an anomaly flagged by a system therefore warrants further examination but does not, by itself, prove that a transaction or an officer's conduct was unlawful.

AI does not, however, guarantee the elimination of corruption: manipulation of data or criteria, or selective use of algorithmic alerts, may create new opportunities for abuse [42]. Material decisions therefore require verifiable outputs, documentation of their use and independent human judgment. Employee monitoring must also respect constitutional safeguards protecting personal information (Article 32(2) of the Constitution of Ukraine) [40].

The third tier is internal corporate regulation. Internal instruments can most promptly define permitted uses of AI, the allocation of powers, system suitability assessments, incident-response procedures and conditions for discontinuing use [2, pp. 115–117; 30]. This approach is consistent with the Federal Court of Australia's observations in *ASIC v Bekier*: the Court regarded deliberate regulation of AI use by boards through the formal adoption of relevant policies as prudent [35, paragraph 394].

For moderate-risk uses, wider reliance on the 'comply or explain' principle is appropriate. This approach is characteristic of contemporary corporate governance codes and preserves organisational freedom while ensuring accountability [13, pp. 34–37; 19; 30; 33, section V]. Regulatory sandboxes are also justified for novel uses of AI [22, pp. 370–372; 23; 32].

The proposed model combines statutory safeguards for high-risk systems, sector-specific regulation reflecting the particular features of each market, and corporate autonomy concerning risks that can be adequately managed internally.

5. Four Regimes of Corporate AI Use

For the practical application of the proposed approach, AI use should be assessed against four criteria.

The first is system autonomy: the scope of actions a system can undertake without a separate human decision [6, pp. 855–861; 21, pp. 2–4].

The second is the materiality of the decision for the company's financial position, the powers of corporate bodies and the rights of its participants. Decisions reserved to the exclusive competence of the general meeting or supervisory board are generally of heightened legal significance [24, Articles 39 and 71; 34, Article 30].

The third is external risk: the potential for substantial adverse effects on the rights of consumers, employees, investors and creditors, personal data protection, competition or market stability, taking account of Articles 24, 32, 42 and 43 of the Constitution of Ukraine [40; 15, Article 9 and Annex III].

The fourth is controllability: the ability to verify the material grounds for an output, reconstruct how the system was used, stop or correct its actions and identify the responsible party.

The initial regime is determined by the most significant risk, taking account of system autonomy, decision materiality and potential effects on third parties. Decision materiality is considered when assessing whether a system is material and determining the required level of human oversight.

Insufficient controllability requires stronger safeguards within the initial regime, restrictions on autonomy or reassignment to a stricter regime. If meaningful oversight cannot be ensured, the system should not be used for the operation in question. High controllability does not lower the initial regime or binding statutory requirements, but may justify broader autonomy for individual operations within that regime. The systemic regime requires a combination of substantial external risk, high autonomy and a potential effect on financial stability or other socially significant interests. The author's classification does not supersede risk classifications established by law.

On this basis, four regimes should be distinguished.

The basic regime applies to systems that are not material within the meaning set out in Section 2. Requirements are established by an internal instrument: rules for use and an appropriate level of user awareness.

The enhanced regime applies to material systems whose use does not create significant external risk; their outputs must be subject to substantive review by an authorised person. It operates primarily at the corporate level and entails system registration, risk assessment, designation of a responsible person and periodic review.

The significant-external-risk regime applies to material systems posing significant external risks, particularly to the rights of consumers, employees, investors or creditors, and is not equivalent to the classification of high-risk systems under Regulation (EU) 2024/1689. Where a system is classified as high-risk under applicable law, including Regulation (EU) 2024/1689 in circumstances falling within Article 2, mandatory requirements apply irrespective of the company's own risk assessment [15, Articles 2 and 6; Annex III]. Legally binding requirements for such systems must be established by legislation or, pursuant to legislation, by an instrument of an authorised regulator [40, Article 19(2), Article 92(1)(8)]. This regime may encompass prior impact assessment, suitability testing independent of system developers, effective human oversight, documentation of material actions and oversight by the competent corporate body.

The systemic regime applies to highly autonomous AI systems whose use creates significant external risk and may affect financial stability or other socially significant interests. In addition to the safeguards of the significant-external-risk regime, it may involve external review, notification of material incidents to the regulator and special public supervision on grounds established by law.

Irrespective of the regime, AI outputs used to prepare decisions reserved to the exclusive competence of a corporate body must undergo substantive review before the relevant decision is adopted.

These proposed regimes are doctrinal in nature: they do not replace statutory risk classifications or create new legal obligations.

Conclusions

AI may perform a wide range of functions in corporate governance—from analysing information and preparing decision options to carrying out individual operations within defined limits—but cannot acquire the competence of a corporate body. Decisions reserved to the exclusive competence of corporate bodies must be made by those bodies, not by AI systems.

AI use does not change the grounds of officers' liability, but affects what their duty to act carefully and professionally entails. To organise AI use appropriately, a company should maintain an inventory of material systems, assess their risks, designate

responsible persons and review outputs. Uncritical reproduction of a system's conclusions may indicate improper performance of duties. Records of substantive review may help demonstrate that an officer has properly discharged their duties.

Public supervision of AI use is subject to constitutional limits: restrictions are permissible only where they have a legal basis, pursue a legitimate aim and are proportionate. Regulators should therefore primarily assess the adequacy of risk management systems and decision-making procedures rather than the expediency of business choices. Within the scope of public supervision, the substance of a decision remains reviewable for compliance with law and third-party rights. This does not restrict internal corporate oversight exercised by participants and supervisory boards. Legal regulation of AI in corporate governance should be proportionate to risk and respect the limits of corporate autonomy. Legislation should establish safeguards for high-risk systems; regulators should specify requirements for their respective markets within the powers conferred by law; and companies may address other matters through internal instruments. The extent of requirements should depend on system autonomy, decision materiality, external risk and the possibility of human oversight, rather than on AI use as such.

Properly organised AI use can reduce corruption risks, particularly in state-owned enterprises and companies with state participation, by identifying conflicts of interest and improving decision-making transparency. At the same time, manipulation of data and algorithmic criteria or selective reliance on system alerts can create new opportunities for abuse. Such tools therefore require verifiability, human oversight and protection of employees' rights. A promising subject for further research is the liability of legal entities for the actions of agentic AI systems.

Declaration on the Use of Artificial Intelligence

In preparing this article, ChatGPT was used as an auxiliary tool for editorial and linguistic revision, checking logical and terminological consistency, identifying possible inaccuracies and developing editorial suggestions. The author determined the scientific conclusions, legal assessments and final version of the article and assumes responsibility for its content.

References

1. Saloid S., Khlebynska O. Legal Regulation of the Use of Artificial Intelligence in Organisational Management: Managerial Risks and Compliance. *Current Issues in Economic Sciences*. 2026. No. 23. DOI: 10.5281/zenodo.20713889. URL: <https://www.a-economics.com.ua/index.php/home/article/download/1647/1612> (accessed 19 October 2026). (in Ukrainian)
2. Zozuliak O., Paruta Yu. Theoretical and Legal Aspects of Identifying Trends in Corporate Governance Development in Ukraine. *Art of Justice*. 2025. Issue 1 (32). Pp. 112–118. DOI: 10.33098/3083-726X.2025.1.32.112-118. URL: <https://aj.ukd.edu.ua/index.php/journal/article/download/15/13> (accessed 19 October 2026). (in Ukrainian)
3. Kourabas S., Tsang C.-Y. The Board Monitoring Function: Artificial Intelligence in the Era of Heightened Accountability. *ECGI Law Working Paper*. 2025. No. 856/2025. 36 p. URL: <https://www.ecgi.global/sites/default/files/2025-07/the-board-monitoring-function-artificial-intelligence-in-the-era-of-heightened-accountability.pdf> (accessed 19 October 2026).
4. Ferreira D., Li J. Artificial Intelligence in the Boardroom. *ECGI Finance Working Paper*. 2025. No. 1087/2025. 65 p. Revised Apr. 2026. URL: <https://www.ecgi.global/sites/default/files/2026-04/artificial-intelligence-in-the-boardroom.pdf> (accessed 19 October 2026).
5. Lipianina-Honcharenko Kh., Komar M., Bykovyi P., Yurkiv Kh. Corporate Governance of Responsible Artificial Intelligence in Leading IT Corporations: A Comparative Analysis of Principles, Internal Standards and Practices. *Measuring and Computing Devices in Technological Processes*. 2026. No. 2. Pp. 364–373. DOI: 10.31891/2219-9365-2026-86-43. URL: <https://vottp.khmnu.edu.ua/index.php/vottp/article/view/790/831> (accessed 19 October 2026). (in Ukrainian)
6. Hilb M. Toward Artificial Governance? The Role of Artificial Intelligence in Shaping the Future of Corporate Governance. *Journal of Management and Governance*. 2020. Vol. 24. P. 851–870. DOI: 10.1007/s10997-020-09519-9. URL:

<https://link.springer.com/content/pdf/10.1007/s10997-020-09519-9.pdf> (accessed 19 October 2026).

7. Petrin M. AI Accountability from the Outside In: Corporate Liability, AI Governance, and Managerial Duties. ECGI Law Working Paper. 2026. No. 935/2026. 27 p. URL: <https://www.ecgi.global/sites/default/files/2026-06/6709258.pdf> (accessed 19 October 2026).

8. Gan K. C. J., Wilczek-Stronczek B., Papasava A. Governing the Algorithm: A Conceptual Review of Strategic AI Oversight in Global Corporations. AI & Society. 2026. DOI: 10.1007/s00146-026-03207-2. URL: <https://link.springer.com/content/pdf/10.1007/s00146-026-03207-2.pdf> (accessed 19 October 2026).

9. Zhornokui Yu. A Comparative Analysis of the Legal Personality of a Legal Entity and Artificial Intelligence in the Context of Their Influence on Corporate Governance. Civil Law Platform. 2024. No. 3. Pp. 98–112. DOI: 10.69724/2786-8834-2024-3-3-98-112. URL: <https://clp.org.ua/wp-content/uploads/2024/02/zhornokuj-iurij.-porivnialnyj-analiz-pravosub-iektnosti-iurydychnoi-osoby-ta-shtuchnoho-intelektu-u-konteksti-vplyvu-na-korporativne-upravlinnia.pdf> (accessed 19 October 2026). (in Ukrainian)

10. Sishchuk L. V. Application of Artificial Intelligence in Corporate Governance. Forum Prava. 2025. Vol. 84, No. 4. Pp. 76–83. DOI: 10.5281/zenodo.17347717. URL: https://repository.ndippp.gov.ua/bitstream/handle/765432198/1189/%D0%A1%D1%96%D1%89%D1%83%D0%BA_%D0%A8%D0%86_%D0%B2_%D0%9A%D0%A3.pdf?isAllowed=y&sequence=1 (accessed 19 October 2026). (in Ukrainian)

11. Möslin F. European Company Law in the Age of Digital Transformation: Artificial Intelligence, Data Economy, and Digital Corporate Governance. ERA Forum. 2025. Vol. 26. P. 629–646. DOI: 10.1007/s12027-025-00864-6. URL: <https://link.springer.com/content/pdf/10.1007/s12027-025-00864-6.pdf> (accessed 19 October 2026).

12. Chiu I. H.-Y., Lim E. W. K. Managing Corporations' Risk in Adopting Artificial Intelligence: A Corporate Responsibility Paradigm. Washington University Global Studies Law Review. 2021. Vol. 20, No. 2. P. 347–389. URL:

<https://journals.library.wustl.edu/globalstudies/article/8690/galley/25488/view>

(accessed 19 October 2026).

13. Rousseau S., Régis C. Artificial Intelligence and the Board of Directors: AI Governance Frameworks and Disclosure Practices of Canadian-Listed Corporations. University of Montreal Faculty of Law Research Paper. 2026. 41 p. Forthcoming in Cambridge Forum on AI: Law and Governance. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6974198 (accessed 19 October 2026).

14. INSEAD Corporate Governance Centre, KPMG International. AI Governance Principles for Boards. Fontainebleau : INSEAD, 2026. 22 p. URL: <https://www.insead.edu/system/files/2026-04/ai-principles-for-boards-report-2026.pdf> (accessed 19 October 2026).

15. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Official Journal of the European Union. 2024. L 2024/1689. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689. As amended by Regulation (EU) 2026/1744 (OJ L, 24.07.2026; URL: <https://eur-lex.europa.eu/eli/reg/2026/1744/oj>) (accessed 19 October 2026).

16. Tabassi E. Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD : National Institute of Standards and Technology, 2023. 48 p. DOI: 10.6028/NIST.AI.100-1. URL: <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf> (accessed 19 October 2026).

17. Organisation for Economic Co-operation and Development. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449. Adopted 22 May 2019; amended 3 May 2024. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> (accessed 19 October 2026).

18. Hickman E., Petrin M. Trustworthy AI and Corporate Governance: The EU's Ethics Guidelines for Trustworthy Artificial Intelligence from a Company Law Perspective.

- European Business Organization Law Review. 2021. Vol. 22. P. 593–625. DOI: 10.1007/s40804-021-00224-0. URL: <https://link.springer.com/content/pdf/10.1007/s40804-021-00224-0.pdf> (accessed 19 October 2026).
19. Financial Reporting Council. Corporate Governance Code Guidance. Published 29 January 2024; last updated 3 June 2026. London : Financial Reporting Council, 2026. URL: <https://www.frc.org.uk/library/standards-codes-policy/corporate-governance/corporate-governance-code-guidance> (accessed 19 October 2026).
20. Matera P. From Red Flags to Black Boxes: Corporate Oversight in the Age of Artificial Intelligence. St. John's Law Review. 2026. Vol. 100 (forthcoming). 62 p. DOI: 10.2139/ssrn.6161886. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6161886 (accessed 19 October 2026).
21. Petrin M. When AI Hurts: Corporate Responsibility for Agentic AI. Harvard Journal of Law & Technology. 2026. Vol. 40 (forthcoming). 27 p. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=6814644 (accessed 19 October 2026).
22. Bello y Villarino J.-M., Bronitt S. AI-Driven Corporate Governance: A Regulatory Perspective. Griffith Law Review. 2024. Vol. 33, No. 4. P. 355–374. DOI: 10.1080/10383441.2024.2405752. URL: <https://www.tandfonline.com/doi/full/10.1080/10383441.2024.2405752> (accessed 19 October 2026).
23. National Bank of Ukraine. Discussion Paper on the Ethical and Responsible Use of Artificial Intelligence by Participants in the Ukrainian Financial Services Market. Kyiv: National Bank of Ukraine, 2026. 20 pp. URL: https://bank.gov.ua/admin_uploads/article/Discussion_paper_AI-2026-03-24.pdf?v=19 (accessed 19 October 2026). (in Ukrainian)
24. Law of Ukraine No. 2465-IX of 27 July 2022, On Joint Stock Companies. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/go/2465-20> (accessed 19 October 2026). (in Ukrainian)

25. Law of Ukraine No. 1953-IX of 14 December 2021, On Financial Services and Financial Companies. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/go/1953-20> (accessed 19 October 2026). (in Ukrainian)
26. Law of Ukraine No. 3480-IV of 23 February 2006, On Capital Markets and Organised Commodity Markets. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/go/3480-15> (accessed 19 October 2026). (in Ukrainian)
27. National Bank of Ukraine Board Resolution No. 64 of 11 June 2018, On Approval of the Regulation on the Organisation of Risk Management Systems in Banks of Ukraine and Banking Groups. Official Website of the National Bank of Ukraine. URL: https://bank.gov.ua/ua/legislation/Resolution_11062018_64 (accessed 19 October 2026). (in Ukrainian)
28. National Bank of Ukraine Board Resolution No. 185 of 27 December 2024, On Approval of the Regulation on Requirements for the Corporate Governance and Internal Control Systems of Financial Companies and Amendments to Certain Regulatory Acts of the National Bank of Ukraine. Official Website of the National Bank of Ukraine. URL: https://bank.gov.ua/ua/legislation/Resolution_27122024_185 (accessed 19 October 2026). (in Ukrainian)
29. National Bank of Ukraine Board Decision No. 814-rsh of 3 December 2018, On Approval of Methodological Recommendations on Corporate Governance Arrangements in Ukrainian Banks. Official Website of the National Bank of Ukraine. URL: https://bank.gov.ua/ua/legislation/Decision_03122018_814-rsh (accessed 19 October 2026). (in Ukrainian)
30. National Securities and Stock Market Commission. Corporate Governance Code: Key Requirements and Recommendations. Approved by Decision No. 118 of 12 March 2020. 48 pp. URL: <https://www.nssmc.gov.ua/documents/kodeks-korporatyvnoho-upravlinnia-kliuchovi-vymohy-i-rekomendatsii> (accessed 19 October 2026). (in Ukrainian)
31. Cabinet of Ministers of Ukraine Order No. 1351-r of 31 December 2024, On Endorsement of the Strategy for Digital Development of Innovation Activities in

Ukraine until 2030 and Approval of the Operational Action Plan for 2025–2027. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/go/1351-2024-%D1%80> (accessed 19 October 2026). (in Ukrainian)

32. Ministry of Digital Transformation of Ukraine. White Paper on AI Regulation in Ukraine: The Ministry's Vision. Consultation Version. Kyiv, 2024. 30 pp. URL: <https://storage.thedigital.gov.ua/files/a/ba/d5da75c2613e331bb89258f950adcbae.pdf> (accessed 19 October 2026). (in Ukrainian)

33. OECD. G20/OECD Principles of Corporate Governance 2023. Paris : OECD Publishing, 2023. 53 p. DOI: 10.1787/ed750b30-en. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/09/g20-oecd-principles-of-corporate-governance-2023_60836fcb/ed750b30-en.pdf (accessed 19 October 2026).

34. Law of Ukraine No. 2275-VIII of 6 February 2018, On Limited and Additional Liability Companies. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/go/2275-19> (accessed 19 October 2026). (in Ukrainian)

35. Australian Securities and Investments Commission v Bekier (Liability Judgment) [2026] FCA 196 : judgment of the Federal Court of Australia, Lee J, 5 March 2026. URL: <https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2026/2026fca0196> (accessed 19 October 2026).

36. Civil Code of Ukraine No. 435-IV of 16 January 2003. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/laws/show/435-15> (accessed 19 October 2026). (in Ukrainian)

37. Bernaziuk I. M. Artificial Intelligence in Banking: Constitutional Guarantees of Customer Rights and a Risk-Based Model of Legal Regulation in Ukraine. Konstytutsionalist. 2026. URL: <https://constitutionalist.com.ua/shtuchnyj-intelekt-u-bankivskij-diialnosti-konstytutsijni-harantii-prav-kliienta-ta-ryzyk-orientovana-model-pravovoho-rehuliuвання-v-ukraini> (accessed 19 October 2026). (in Ukrainian)

38. Bernaziuk I. M. Artificial Intelligence in Insurance: Legal Limits of Algorithmic Risk Assessment, Pricing and Decisions on Insurance Claims. *Konstytutsionalist*. 2026. URL: <https://constitutionalist.com.ua/shtuchnyj-intelekt-u-strakhuvanni-pravovi-mezhi-alhorytmichnoho-otsiniuvannia-ryzyku-tsinoutvorennia-ta-pryjniattia-rishen-shchodo-strakhovykh-vyplat> (accessed 19 October 2026). (in Ukrainian)
39. Bernaziuk I. M. Artificial Intelligence in the Operation of the Institution of Lobbying in Ukraine: Constitutional Principles of Transparency and the Prevention of Improper Influence. *Konstytutsionalist*. 2026. URL: <https://constitutionalist.com.ua/shtuchnyj-intelekt-u-funktsionuvanni-instytutu-lobiiuvannia-v-ukraini-konstytutsijni-zasady-prozorosti-ta-zapobihannia-nepravomirnomu-vplyvu> (accessed 19 October 2026). (in Ukrainian)
40. Constitution of Ukraine No. 254k/96-VR of 28 June 1996. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/go/254%D0%BA/96-%D0%B2%D1%80> (accessed 19 October 2026). (in Ukrainian)
41. Grand Chamber of the Supreme Court of Ukraine. Judgment of 25 May 2021 in Case No. 910/11027/18 (Proceedings No. 12-185rc19). URL: <https://reyestr.court.gov.ua/Review/98235845> (accessed 19 October 2026). (in Ukrainian)
42. Köbis N., Starke C., Rahwan I. The Promise and Perils of Using Artificial Intelligence to Fight Corruption. *Nature Machine Intelligence*. 2022. Vol. 4, No. 5. P. 418–424. DOI: 10.1038/s42256-022-00489-1. URL: <https://doi.org/10.1038/s42256-022-00489-1> (accessed 19 October 2026).
43. Law of Ukraine No. 1700-VII of 14 October 2014, On Prevention of Corruption. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/go/1700-18> (accessed 19 October 2026). (in Ukrainian)
44. Second Senate of the Constitutional Court of Ukraine. Decision No. 9-r(II)/2023 of 1 November 2023, on the Constitutional Complaint of Nataliia Tryhub (Individualisation of Legal Liability for Violations of Consumer Rights). URL: <https://ccu.gov.ua/dokument/9-rii2023> (accessed 19 October 2026). (in Ukrainian)

45. Bernaziuk I. M. Artificial Intelligence in the Prevention of Corruption in Ukraine: Constitutional Limits and Preventive Potential. Konstitutsionalist. 2026. URL: <https://constitutionalist.com.ua/shtuchnyj-intelekt-u-systemi-zapobihannia-koruptsii-v-ukraini-konstytutsijni-mezhi-ta-preventyvnyj-potentsial> (accessed 19 October 2026). (in Ukrainian)
46. Law of Ukraine No. 3587-IX of 22 February 2024, On Amendments to Certain Legislative Acts of Ukraine Concerning Improvements in Corporate Governance. Legislation of Ukraine Database, Verkhovna Rada of Ukraine. URL: <https://zakon.rada.gov.ua/laws/show/3587-20> (accessed 19 October 2026). (in Ukrainian)
47. Corporations Act 2001 (Cth) : Australian Government, Federal Register of Legislation. URL: <https://www.legislation.gov.au/C2004A00818/latest/text> (accessed 19 October 2026).