Review scientific paper DOI: 10.56461/iup_rlrc.2026.7.ch4

Dávid MOLNÁR*

FROM COMPLIANCE TO STATE CAPACITY: AI REGULATION IN THE EU AND UAE

Rapid advances in artificial intelligence challenge the capacity of legal systems to regulate emerging technologies without undermining innovation. This paper examines two contrasting regulatory paradigms in public and private law: the compliance-oriented model of the European Union and the governance-driven approach of the United Arab Emirates. The EU framework is characterized by ex ante risk classification, horizontal regulation, and strong rights-based safeguards, aiming to mitigate systemic risks but often increasing regulatory friction, while the Emirati model relies on centralized coordination, regulatory sandboxes, and adaptive legal instruments that integrate artificial intelligence into state capacity and economic policy. The paper proceeds from the hypothesis that the design of regulation influences the pace of innovation, the level of legal certainty, and the extent to which artificial intelligence becomes a tool of public authority and private economic growth, arguing that AI regulation is no longer merely a question of legal restraint but of strategic governance. The research is conducted using a comparative method, a normative-dogmatic method, and a content analysis method.

Keywords: artificial intelligence regulation, public law, private law, EU, UAE.

1. INTRODUCTION

The vertiginous and inexorably accelerative ontogenesis of artificial intelligence systems, manifesting in epistemic opacity conjoined with near-limitless scalability and an inherent duality of emancipatory telos and latent perniciousness, has caught our legal architectures somewhat off guard. What began as a seemingly benign wave of technological exuberance has swiftly unmasked the structural limitations of many of our erstwhile normative instruments when confronted with phenomena that defy perspicuous interpretation while oscillating precariously between societal amelioration and substantial individual and collective harm (Ebers, 2025, pp. 684–689; Rangone & Megale, 2025, pp. 1082–1087; Bignami *et al*., 2025; Basu & Dave, 2025).

* University of Pécs, Faculty of Law, Hungary, ORCID: https://orcid.org/0009-0000-5836-4825, e-mail: *molnardavid836@gmail.com*

As these developments have unfolded, the pecuniary vector has assumed an especially salient valence. By 2025, the global artificial intelligence market had burgeoned to a valuation of USD 390.91 billion, with extrapolations forecasting an ascent to USD 3,497.26 billion by 2033 at a compound annual growth rate of 30.6 percent (Grand View Research, 2025). Contemporaneous econometric prognostications from IDC anticipate that investments in AI solutions and ancillary services may precipitate a cumulative global economic imprint exceeding USD 22.3 trillion by 2030—an increment tantamount to approximately 3.7 percent of projected global GDP—thereby amplifying apprehensions surrounding algorithmic partiality, the erosion of informational privacy and broader societal transformation (International Data Corporation, 2025; Graux *et al.*, 2025, pp. 8–12).

These impressive metrics, while ostensibly evincing prodigious latent capacity for augmenting operational efficiencies, concurrently intensify concerns regarding algorithmic partiality, informational privacy erosion and broader societal metamorphoses (Ebers, 2025, pp. 684–689; Rangone & Megale, 2025, pp. 1082–1087). Different jurisdictions, attuned to their idiosyncratic governmental morphologies, economic imperatives and geopolitical exigencies, articulate responses that evince substantial regulatory heterogeneity (Bignami *et al.*, 2025; Albous, Al-Jayyousi & Stephens, 2025, pp. 2389–2396).

Two conspicuously antithetical paradigms of AI governance command particular scholarly exegesis. The European Union has promulgated a meticulously architected, compliance-centric edifice through Regulation (EU) 2024/1689, denominated the Artificial Intelligence Act, which attained juridical efficacy on 1 August 2024 (European Parliament and Council of the European Union, 2024, Art. 113). This instrument delineates a quadripartite taxonomy of risk—unacceptable, high, limited and minimal—whilst superimposing incrementally stringent obligations across the entirety of the AI lifecycle. It proscribes practices such as specified forms of social scoring and manipulative techniques, while encumbering high-risk modalities with strictures encompassing risk-management protocols, data-governance regimes, transparency imperatives, conformity assessments and human supervisory mechanisms (European Parliament and Council of the European Union, 2024, Arts. 5–6, 9–15, 43; Ebers, 2025, pp. 684–689).

Interwoven symbiotically with the General Data Protection Regulation and the EU Charter of Fundamental Rights, the framework accords pre-eminence to the safeguarding of individual entitlements and the exigencies of democratic accountability (European Parliament and Council of the European Union, 2024, Art. 1; Graux *et al.*, 2025, pp. 20–21). The quantum of compliance exigencies—preliminary assessments of the Commission's original proposal estimated cumulative economy-wide costs of approximately EUR 31 billion over five years and compliance expenditure of up to EUR 400,000 for an SME introducing a single high-risk AI product requiring a quality-management system—provokes well-founded reservations that, while potentially fortifying societal fiducia in the longue durée, they simultaneously portend regulatory encumbrances capable of attenuating innovation velocity amid an epoch of escalating transnational technological contestation (Mueller, 2021, p. 3; Ebers, 2025, pp. 692–697).

By stark juxtaposition, the United Arab Emirates has embraced a more protean, capacity-augmenting modality predicated upon the UAE National Strategy for Artificial Intelligence 2031, announced in 2017 (United Arab Emirates, 2017, pp. 8–11). Orchestration emanates centrally from the Minister of State for Artificial Intelligence and the UAE Artificial Intelligence and Blockchain Council, buttressed by industry pilots and predominantly hortatory ethical

precepts, inclusive of the 2024 UAE AI Charter. Eschewing a predominantly prohibitive orientation, this paradigm conceptualises AI as a pivotal catalyst for economic diversification, amelioration of public services and augmentation of human capital, with projected opportunities encompassing up to AED 335 billion in additional economic output (United Arab Emirates, 2017, pp. 10–11; United Arab Emirates, 2024).

The celerity of uptake furnishes corroborative evidence: by the terminus of 2025, approximately 64 percent of the UAE's working-age population engaged with generative AI—the highest rate among the jurisdictions examined—with pervasive integration observable within governmental and economic structures (Microsoft AI Economy Institute, 2026, p. 6).

At the same time, the lighter accountability mechanisms raise legitimate concerns regarding weaker enforcement and the risk of "ethics washing" in a predominantly soft-law environment (Albous, Al-Jayyousi & Stephens, 2025, pp. 2413–2414). This divergence raises the central question explored in this article: how do these contrasting regulatory philosophies—one centred on strict ex ante compliance and the other on strategic capacity-building—affect the pace of AI innovation, the degree of legal certainty and the way artificial intelligence evolves into a tool that serves both public power and private economic growth?

AI regulation has manifestly transcended the circumscribed ambit of risk attenuation, metamorphosing into a strategic vector of statecraft within the digital epoch. The EU modality, by privileging robust safeguards, cultivates societal fiducia and normative consonance, albeit at the potential cost of administrative encumbrances that may retard deployment. Conversely, the UAE modality demonstrates considerable efficacy in expediting assimilation and pursuing economic dividends, whilst nonetheless eliciting pertinent interrogations concerning enforcement vigour and congruence with nascent international benchmarks (Ebers, 2025, pp. 695–697; Albous, Al-Jayyousi & Stephens, 2025, pp. 2413–2414; Rangone & Megale, 2025, pp. 1094–1097).

2. THE EUROPEAN UNION'S COMPLIANCE-ORIENTED MODEL

The European Union's regulatory response to artificial intelligence constitutes one of the most ambitious and philosophically charged attempts in contemporary legal history to impose a coherent horizontal order upon a technology that inherently resists easy categorisation. The architecture of Regulation (EU) 2024/1689 reflects a deliberate and almost constitutional ambition: not merely to mitigate risk, but to embed the telos of democratic dignity and fundamental rights within algorithmic systems themselves (European Parliament and Council of the European Union, 2024, Art. 1; Bignami *et al.*, 2025; Rangone & Megale, 2025, pp. 1082–1087). This ambition, however, raises a critical question: does such an extensive framework strengthen the rule of law, or does it risk constraining innovation through an expanding system of ex ante obligations (Ebers, 2025, pp. 684–689; Graux *et al.*, 2025, pp. 8–12)?

2.1. The Artificial Intelligence Act: Risk Classification and Horizontal Regulation

At its core, the Act establishes a quadripartite taxonomy of risk—unacceptable, high, limited and minimal—forming the normative foundation of the regime (European Parliament and Council of the European Union, 2024, Recital 26 and Arts, 5–6; Smuha, 2025, pp. 1238–1245; Ebers, 2025, pp. 684–686). Unacceptable-risk practices, such as specified forms of social

scoring and manipulative or deceptive techniques, are subject to categorical prohibition. This reflects a clear policy judgment that certain applications are incompatible with fundamental rights protected under the EU Charter of Fundamental Rights and the European Convention on Human Rights (European Parliament and Council of the European Union, 2024, Art. 5; Rangone & Megale, 2025, pp. 1082–1087).

High-risk systems—the regulatory centrepiece—include applications in employment, education, law enforcement, migration, access to essential public and private services and the administration of justice, as specified in Annex III. Providers and deployers are subject to extensive ex ante obligations, including risk-management systems, data-governance requirements, transparency obligations, conformity assessments and human-oversight mechanisms (European Parliament and Council of the European Union, 2024, Arts. 6, 9–15, 26, 43, Annex III; Graux *et al*., 2025, pp. 20–21). These obligations collectively establish a normative framework designed to preserve human control, dignity and equality.

The relationship with the General Data Protection Regulation is particularly significant. The AI Act builds upon and operates alongside GDPR principles such as transparency, accountability, data quality and the protection of affected individuals. The interaction is especially apparent where certain deployers must conduct a fundamental-rights impact assessment under Article 27 of the AI Act while also being required to undertake a data protection impact assessment under Article 35 GDPR. Differences in scope, risk classification and supervisory procedure may consequently create duplication and uncertainty for regulated organisations (European Parliament and Council of the European Union, 2024, Art. 27; van Kolfschooten & van Oirschot, 2024; Graux *et al*., 2025, pp. 31–35).

Financial implications are considerable. An assessment of the European Commission's original proposal estimated that the contemplated regime could impose approximately EUR 31 billion in aggregate costs on the European economy over five years and reduce investment in AI by almost 20 percent. It further estimated that an SME introducing one high-risk AI product requiring a quality-management system could face compliance costs of up to EUR 400,000 (Mueller, 2021, p. 3). These figures preceded the adoption of the final Regulation and should therefore be treated as projections concerning the Commission's proposal rather than measured costs of the AI Act in its present form. Nevertheless, they reflect a clear trade-off: enhanced legal certainty and rights protection on one side, and potential constraints on innovation and competitiveness on the other (Ebers, 2025, pp. 692–697; Graux *et al*., 2025, pp. 8–12).

2.2. Strengths, Limitations and Broader Implications

The principal strength of the EU model lies in its commitment to rights protection and legal certainty. By relying on ex ante regulation rather than exclusively upon ex post liability, the framework seeks to prevent harm before it occurs and to foster trust in AI systems (European Parliament and Council of the European Union, 2024, Arts. 5, 9–15, 27; Ebers, 2025, pp. 684–689). Its extraterritorial scope—applying in specified circumstances to providers and deployers established outside the Union—further reinforces its ambition to establish influential regulatory standards similar to the impact of the General Data Protection Regulation (European Parliament and Council of the European Union, 2024, Art. 2; Stampernas & Lambrinoudakis, 2025).

However, significant limitations remain. Compliance costs and administrative burdens may create a chilling effect, particularly for smaller innovators, potentially discouraging

investment or delaying beneficial AI deployment within the European Union. The assessment of the original proposal projected that AI investment could decline by almost 20 percent, although this estimate should not be treated as evidence of the final Regulation's actual economic effects (Mueller, 2021, p. 3). Moreover, the simultaneous application of the AI Act, GDPR, Digital Services Act, Data Act and cybersecurity legislation may produce duplicative, inconsistent or unclear requirements, disproportionately affecting SMEs and start-ups with limited compliance capacity (Graux *et al*., 2025, pp. 8–12).

Future judicial interpretation—especially preliminary references to the Court of Justice of the European Union concerning the scope of high-risk obligations and the balance between innovation and fundamental rights—will play a decisive role in shaping the effectiveness of the framework. Experience under EU data-protection law, including the Court's approach to fundamental rights and international data transfers in Schrems II, demonstrates the significant role that judicial review may assume in defining the territorial reach and substantive requirements of European digital regulation (*Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, 2020).

Ultimately, the EU model reflects a fundamental normative choice: technological progress must not come at the expense of human dignity and democratic accountability. While it enhances legal certainty and societal trust, it may also slow innovation and affect global competitiveness where compliance requirements are applied too rigidly or without sufficient regard to the benefits and actual risks of individual systems. Whether this balance proves sustainable remains an open question in contemporary legal scholarship (Ebers, 2025, pp. 692–703; Rangone & Megale, 2025, pp. 1092–1097; Graux *et al*., 2025, pp. 78–82).

3. THE UNITED ARAB EMIRATES' GOVERNANCE-DRIVEN APPROACH

The United Arab Emirates has deliberately chosen a governance-driven model that treats artificial intelligence less as a risk to be tightly contained and more as a strategic instrument for enhancing state capacity and accelerating economic transformation. This approach prioritises rapid integration and developmental outcomes over comprehensive ex ante prohibitions. It reflects a conscious policy choice to harness artificial intelligence as a tool of national development rather than primarily as an object of regulatory restraint. The model is characterised by a layered structure combining centralised strategic direction with flexible implementation, creating a dynamic feedback loop not replicated in more uniform horizontal regulatory systems (United Arab Emirates, 2017, pp. 8–11; Albous, Al-Jayyousi & Stephens, 2025, pp. 2398–2400).

3.1. National AI Strategy and Institutional Framework

The foundation of the Emirati model is the UAE National Strategy for Artificial Intelligence 2031 (استراتيجية الإمارات للذكاء الاصطناعي 2031), announced in 2017 and elaborated in the national strategy document issued in 2018 (United Arab Emirates, 2017, pp. 8–11). The strategy reflects a broader conception of artificial intelligence as a unified national project. In this context, technological development is closely linked to long-term state-building, economic diversification, public-sector modernisation and the development of educational and social opportunities (United Arab Emirates, 2017, pp. 8–11).

At the structural level, the framework operates across multiple layers. At the micro level, federal and local entities retain flexibility to adapt implementation to their institutional and

sectoral priorities. At the macro level, the UAE presents itself as a coherent actor in global technological governance, coordinated through the Minister of State for Artificial Intelligence and the UAE Artificial Intelligence and Blockchain Council (United Arab Emirates, 2017, pp. 8–11; Albous, Al-Jayyousi & Stephens, 2025, pp. 2398–2400).

An additional normative layer is provided by the 2024 UAE Charter for the Development and Use of Artificial Intelligence (officially ميثاق الإمارات للتطوير والاستخدام الأخلاقي للذكاء الاصطناعي). The Charter reflects a form of soft-law instrument grounded in normative commitment rather than comprehensive binding legislative force. This approach allows for flexibility and institutional adaptation while avoiding the rigidity of uniform horizontal statutory regulation (United Arab Emirates, 2024; Albous, Al-Jayyousi & Stephens, 2025, pp. 2413–2414).

At the legislative level, Federal Decree by Law No. 45 of 2021 Concerning the Protection of Personal Data provides the primary federal data-governance framework. Although the PDPL is not an AI-specific statute, it establishes baseline requirements concerning lawful and transparent processing, purpose limitation, data minimisation, accuracy, security and organisational accountability, thereby providing safeguards relevant to AI deployment in the public and private sectors (United Arab Emirates, 2021, Arts 5–8).

Empirical indicators suggest that this model has facilitated rapid adoption. By the end of 2025, approximately 64 percent of the UAE's working-age population had engaged with generative artificial intelligence technologies, placing the country first among the jurisdictions examined in the Microsoft report (Microsoft AI Economy Institute, 2026, p. 6).

3.2. Regulatory Sandboxes, Adaptive Tools and State Capacity

A defining feature of the UAE approach is the use of testbeds, industry pilots and controlled environments for experimentation and iterative development under institutional supervision. Their function is to reduce uncertainty while enabling real-world testing of artificial intelligence systems across sectors such as energy, healthcare, transportation, tourism and public administration (United Arab Emirates, 2017, pp. 10–11).

The broader regulatory ecosystem is characterised by adaptive legal instruments and targeted legislative safeguards. Rather than relying upon a single comprehensive AI statute, the system combines strategic objectives, horizontal data-protection obligations and sector-specific implementation. The PDPL permits personal-data processing where an appropriate legal basis exists, while maintaining protections concerning transparency, security, automated decision-making and high-risk processing (United Arab Emirates, 2021, Arts. 5–8, 13, 18, 20–23; Bahgat, 2025, pp. 8–23).

Federal and emirate-level initiatives further reinforce this structure. The UAE Artificial Intelligence and Blockchain Council coordinates implementation across federal and local entities, enabling national objectives to be translated into projects adapted to specific governmental and sectoral contexts. This demonstrates a decentralised yet coordinated approach to embedding artificial intelligence within national development priorities (United Arab Emirates, 2017, pp. 8–11).

Emerging judicial and administrative practices provide insight into the model's application. The DIFC Courts' Practical Guidance Note No. 2 of 2023 recognises that large language models and generative AI may assist parties in preparing and presenting cases, provided that appropriate human oversight, transparency, verification, confidentiality and professional safeguards are maintained (DIFC Courts, 2023).

The principal strength of the Emirati model lies in its capacity to integrate artificial intelligence into state functions and economic policy, thereby enhancing administrative efficiency and innovation potential. At the same time, the model raises important questions concerning accountability, transparency and the sufficiency of safeguards. The reliance on soft-law instruments and experimental frameworks may lead to inconsistencies in enforcement and potential gaps in rights protection (Albous, Al-Jayyousi & Stephens, 2025, pp. 2413–2414).

In comparative terms, the UAE model reflects a prioritisation of flexibility, speed and state capacity. This entails a trade-off between accelerated innovation and the level of ex ante legal certainty characteristic of more compliance-oriented frameworks. The sustainability of this balance will depend on the continued evolution of institutional oversight and the capacity to adapt regulatory tools in response to emerging risks.

4. COMPARATIVE ANALYSIS: DIVERGENT PARADIGMS AND THEIR IMPLICATIONS

A comparison of the two models reveals not simply surface-level differences but deeper philosophical and practical choices that each one embodies. At the micro level, the first principles underpinning each system reflect fundamentally different conceptions of the relationship between law, technology and human agency. At the macro level, these choices translate into distinct legal architectures, national objectives and long-term governance strategies. The analysis below examines both levels, weighing the respective strengths and risks associated with each model.

4.1. Micro-level First Principles: Rights Containment Versus Strategic Empowerment

At its most fundamental level, the European Union model is based on the principle of rights containment. The Artificial Intelligence Act treats artificial intelligence as a potential source of risk to individual dignity, safety and democratic values, assigning to law the task of establishing clear boundaries through ex ante obligations (European Parliament and Council of the European Union, 2024, Arts. 5–6; Smuha & Yeung, 2025, pp. 228–240; Ebers, 2025, pp. 684–689; Rangone & Megale, 2025, pp. 1082–1087). The four-tier risk taxonomy, the prohibitions on specified forms of social scoring and manipulative techniques, and the detailed requirements for high-risk systems all derive from this principle: technological development must not undermine the human person or the rule of law (European Parliament and Council of the European Union, 2024, Arts. 5, 9–15; *Digital Rights Ireland Ltd v Minister for Communications*, 2014; *S. and Marper v United Kingdom*, 2008; *Tele2 Sverige AB v Post- och telestyrelsen*, 2016; *Big Brother Watch and Others v United Kingdom*, 2021). While this approach is principled and protective, it may also produce a regulatory posture that assumes the necessity of extensive safeguards unless risks are adequately mitigated (Ebers, 2025, pp. 692–697; Graux *et al*., 2025, pp. 8–12).

By contrast, the United Arab Emirates model is grounded in the principle of strategic empowerment. Artificial intelligence is treated not primarily as a risk to be contained but as a lever for enhancing state capacity, economic diversification and national resilience. Strategic frameworks such as the UAE National Strategy for Artificial Intelligence 2031 and the 2024 UAE Charter for the Development and Use of Artificial Intelligence position technology as an instrument of national development. The use of testbeds, industry pilots and the flexible

structure of the PDPL framework reflect a regulatory approach that prioritises experimentation and adaptive governance (United Arab Emirates, 2017, pp. 2–3; United Arab Emirates, 2024; United Arab Emirates, 2021, Arts. 5–8, 13, 18, 20–23). While this model promotes innovation and rapid deployment, it also raises concerns regarding accountability, stakeholder participation and the consistency of safeguards (Albous, Al-Jayyousi & Stephens, 2025, pp. 2413–2414).

4.2. Macro-level Legal Context, Goals and Systemic Learnings

At the macro level, these first principles translate into distinct regulatory strategies. The European Union has developed a horizontal, rights-based framework aimed at establishing consistent standards while protecting fundamental rights. Its objectives include normative coherence, legal certainty and the preservation of democratic values in the digital age. The strength of this approach lies in its structured and legally enforceable character; however, it may also generate regulatory friction, overlapping obligations and potential competitive disadvantages, particularly for smaller enterprises (European Parliament and Council of the European Union, 2024, Art. 1; Ebers, 2025, pp. 692–697; Graux *et al*., 2025, pp. 8–12).

The UAE model, by contrast, is governance-driven and development-oriented. Its primary objective is to utilise artificial intelligence as an engine of economic diversification and state modernisation in a post-oil context. The institutional architecture combines central strategy with implementation by federal and local entities, supported by policy instruments, industry pilots and existing legislation. This structure enables comparatively rapid policy iteration, where experience from practical implementation may inform wider national strategies. Judicial and administrative guidance further contributes to this evolving framework, with instruments such as the DIFC Courts' guidance on generative AI illustrating a pragmatic approach that permits technological assistance while preserving human responsibility, transparency and professional safeguards (United Arab Emirates, 2017, pp. 4–8; Albous, Al-Jayyousi & Stephens, 2025, pp. 2398–2400; DIFC Courts, 2023).

4.3. Mutual Learnings: What Each Model Can Offer the Other

The comparative perspective highlights opportunities for mutual learning. The UAE's adaptive feedback mechanisms may offer the European Union tools to mitigate regulatory rigidity. The use of controlled experimentation, industry pilots, iterative policy development and responsiveness to empirical outcomes could enhance flexibility without necessarily undermining the protection of fundamental rights (United Arab Emirates, 2017, pp. 10–11; Albous, Al-Jayyousi & Stephens, 2025, pp. 2398–2400).

Conversely, elements of the European Union framework may strengthen the UAE model. The EU's structured conformity-assessment procedures and its integration with data-protection and fundamental-rights principles provide robust mechanisms for accountability and oversight. Incorporating elements such as clearer transparency requirements, systematic risk-management procedures and enhanced human oversight into the UAE's strategic and soft-law framework could reduce risks associated with insufficient safeguards, including concerns related to "ethics washing" (European Parliament and Council of the European Union, 2024, Arts. 9–15, 27, 43; Graux *et al*., 2025, pp. 20–21, 31–35; Albous, Al-Jayyousi & Stephens, 2025, pp. 2413–2414).

Neither model is without limitations. The EU prioritises rights protection and legal certainty, potentially at the expense of speed and innovation. The UAE prioritises flexibility and

rapid development, potentially at the expense of long-term accountability and consistency of enforcement. A balanced approach may emerge through hybrid models that combine the EU's normative rigour with the UAE's adaptive capacity. Such a synthesis could provide a viable pathway for jurisdictions seeking to reconcile technological innovation with legal accountability and democratic legitimacy in an increasingly complex regulatory environment.

5. CONCLUSION

The two models examined in this article embody fundamentally different responses to the same core question: what is the proper role of law in regulating a transformative technology such as artificial intelligence? The European Union adopts a model of rights containment, relying on a comprehensive ex ante framework that prioritises the protection of fundamental values, even at the possible cost of regulatory friction and slower innovation (European Parliament and Council of the European Union, 2024, Arts. 1, 5–6, 9–15; Ebers, 2025, pp. 692–697; Graux *et al*., 2025, pp. 8–12). The United Arab Emirates, by contrast, adopts a model of strategic empowerment, characterised by an adaptive and governance-driven approach that treats artificial intelligence as a lever for state capacity and economic diversification, achieving high levels of adoption while raising concerns regarding long-term accountability (United Arab Emirates, 2017, pp. 8–11; Microsoft AI Economy Institute, 2026, p. 6; Albous, Al-Jayyousi & Stephens, 2025, pp. 2413–2414).

Neither model is without limitations. The European Union framework offers normative clarity and legal certainty, yet its compliance burden may create competitive disadvantages. The UAE model enables rapid deployment and practical integration, yet its reliance on flexible and policy-based instruments raises legitimate questions concerning enforcement consistency, stakeholder participation and the risk of "ethics washing" (Ebers, 2025, pp. 692–697; Graux *et al*., 2025, pp. 8–12; Albous, Al-Jayyousi & Stephens, 2025, pp. 2413–2414). These trade-offs suggest that neither purely compliance-oriented nor purely governance-driven approaches provide a complete solution.

A more balanced trajectory may lie in hybrid models that combine the EU's normative rigour with the UAE's adaptive regulatory mechanisms, including feedback loops, controlled experimentation and industry pilots. Such approaches may offer a more effective means of reconciling innovation with accountability in rapidly evolving technological environments.

Ultimately, artificial intelligence regulation has evolved beyond a question of risk management. It has become a strategic dimension of statecraft in the digital age. The regulatory choices made today will shape not only innovation dynamics and legal certainty, but also the broader societal outcomes associated with technological development. Future empirical research on measurable impacts—including productivity gains, investment flows, talent attraction, compliance costs and regulatory convergence—will be essential to inform these choices.

LIST OF REFERENCES

Albous, M.R., Al-Jayyousi, O.R. & Stephens, M. 2025. AI governance in the GCC states: A comparative analysis of national AI strategies. *Journal of Artificial Intelligence Research*, 82, pp. 2389–2422. https://doi.org/10.1613/jair.1.17619

Bahgat, A. 2025. AI governance and data privacy in cross-border contexts: A comparative analysis of regulatory frameworks. *Journal of Data Protection & Privacy*, 8(1), pp. 8–23. https://doi.org/10.69554/BOJL3033

Basu, N. & Dave, R. 2025. Comparative analysis of laws in AI. *Journal of Lifestyle and SDGs Review*, 5(3), e05575. https://doi.org/10.47172/2965-730X.SDGsReview.v5.n03.pe05575

Bignami, E.G. *et al.* 2025. Balancing innovation and control: The European Union AI Act in an era of global uncertainty. *JMIR AI*, 4, e75527. https://doi.org/10.2196/75527

Ebers, M. 2025. Truly risk-based regulation of artificial intelligence: How to implement the EU's AI Act. *European Journal of Risk Regulation*, 16(2), pp. 684–703. https://doi.org/10.1017/err.2024.78

Graux, H. *et al.* 2025. *Interplay between the AI Act and the EU digital legislative framework*. Luxembourg: European Parliament, ECTI_STU(2025)778575. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2025/778575/ECTI_STU(2025)778575_EN.pdf

Rangone, N. & Megale, L. 2025. Risks without rights? The EU AI Act's approach to AI in law and rule-making. *European Journal of Risk Regulation*, 16(3), pp. 1082–1097. https://doi.org/10.1017/err.2025.13

Smuha, N.A. 2025. Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 (EU Artificial Intelligence Act). *International Legal Materials*, 64(5), pp. 1234–1381. https://doi.org/10.1017/ilm.2024.46

Smuha, N.A. & Yeung, K. 2025. The European Union's AI Act: Beyond motherhood and apple pie? In: Smuha, N.A. (ed.), *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence*. Cambridge: Cambridge University Press, pp. 228–258. https://doi.org/10.1017/9781009367783.015

Stampernas, S. & Lambrinoudakis, C. 2025. A framework for compliance with Regulation (EU) 2024/1689 for small and medium-sized enterprises. *Journal of Cybersecurity and Privacy*, 5(3), 40. https://doi.org/10.3390/jcp5030040

van Kolfschooten, H. & van Oirschot, J. 2024. The EU Artificial Intelligence Act (2024): Implications for healthcare. *Health Policy*, 149, 105152. https://doi.org/10.1016/j.healthpol.2024.105152

Reports and internet sources

Grand View Research. 2025. *Artificial Intelligence Market Size, Share & Trends Analysis Report, 2025–2033*. Available at: https://www.grandviewresearch.com (7. 3. 2026).

International Data Corporation (IDC). 2025. *IDC Predicts AI Solutions and Services Will Generate Global Impact of $22.3 Trillion by 2030*. Available at: https://my.idc.com/getdoc.jsp?containerId=prUS53290725 (21. 3. 2026).

Microsoft AI Economy Institute. 2026. *Global AI Adoption in 2025 – A Widening Digital Divide*. Available at: https://www.microsoft.com/en-us/research/wp-content/uploads/2026/01/Microsoft-AI-Diffusion-Report-2025-H2.pdf (25. 3. 2026).

Mueller, B. 2021. *How Much Will the Artificial Intelligence Act Cost Europe?*. Washington, DC: Centre for Data Innovation. Available at: https://www2.datainnovation.org/2021-aia-costs.pdf (18. 3. 2026).

United Arab Emirates. 2017. *UAE National Strategy for Artificial Intelligence 2031*. Abu Dhabi: United Arab Emirates Minister of State for Artificial Intelligence Office. Available at: https://staticcdn.mbzuai.ac.ae/mbzuaiwpprd01/2022/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf (9. 3. 2026).

United Arab Emirates. 2024. *UAE AI Charter (Mīthāq al-Imārāt lil-Dhakāʾ al-Istināʾī)*. Abu Dhabi: Government of the United Arab Emirates. Available at: https://uaelegislation.gov.ae/en/policy/details/the-uae-charter-for-the-development-and-use-of-artificial-intelligence (27. 3. 2026).

Legal sources

European Parliament and Council of the European Union. 2024. Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), *Official Journal of the European Union*, L 235/1. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj (14. 1. 2026).

United Arab Emirates. 2021. Federal Decree-Law No. 45 of 2021 Concerning the Protection of Personal Data (PDPL). Available at: https://uaelegislation.gov.ae/en/legislations/1972/download (14. 1. 2026).

Case law and official documents

Court of Justice of the European Union. 2014. *Digital Rights Ireland Ltd v Minister for Communications*, Joined Cases C-293/12 and C-594/12, Judgment of 8 April 2014.

Court of Justice of the European Union. 2016. *Tele2 Sverige AB v Post- och telestyrelsen*, Joined Cases C-203/15 and C-698/15, Judgment of 21 December 2016.

Court of Justice of the European Union. 2020. *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II)*, Case C-311/18, Judgment of 16 July 2020.

DIFC Courts. 2023. *Practical Guidance Note No. 2 of 2023: Guidelines on the Use of Large Language Models and Generative AI in Proceedings Before the DIFC Courts*. Dubai: DIFC Courts. Available at: https://www.difccourts.ae/rules-decisions/practice-directions/practical-guidance-note-no-2-2023-guidelines-use-large-language-models-and-generative-ai-proceedings-difc-courts (14. 1. 2026).

European Court of Human Rights. 2008. *S. and Marper v United Kingdom*, Applications Nos. 30562/04 and 30566/04, Judgment of 4 December 2008.

European Court of Human Rights. 2021. *Big Brother Watch and Others v United Kingdom*, Applications Nos. 58170/13, 62322/14 and 24960/15, Judgment of 25 May 2021.