Harmonising Consensus: The (Geo)political Economy of Standardisation in the AI Act

by **Marta Cantero Gamito** *

Abstract: This paper examines the broader implications of current global (geo)political dynamics on AI standardisation and how, in turn, standardisation shapes those dynamics. Focusing on the European Union's AI Act, it argues that the Regulation's reliance on delegated technical standards embeds structural and context-dependent vulnerabilities that constrain its ability to project normative influence. Through insights from the political economy of standardisation, the paper explores the interactions between EU and non-EU aspiration and expectations from standards. It contrasts the EU, the US and China approaches and highlights the operational and normative frictions that arise in standard-setting. The findings show an important gap between the EU's regulatory ambitions and the realities of the global standardisation ecosystem, which ultimately raises questions about the long-term coherence and influence of the AI Act in shaping the global AI value chain.

Keywords: AI Act, AI Governance, AI Standardisation, Co-Regulation, Harmonised Standards, EU Law, Geopolitics of Technology, Digital Sovereignty, Strategic Autonomy

Recommended citation: Marta Cantero Gamito, Harmonising Consensus: The (Geo)political Economy of Standardization in the AI ActI, 17 (2026) JIPITEC 75 para 1.

A. Introduction

1 The governance of artificial intelligence (AI) is unfolding in a world marked by the fragmentation of the international legal order and the progressive displacement of rulemaking from states to hybrid, transnational settings. In this shifting landscape, standardisation has emerged as a critical element of AI governance.[1] Beyond its traditional functions of interoperability and market access, standardisation increasingly operates as a mechanism through which regulatory choices are translated into operational requirements. As such, standards play a constitutive role in determining whether political values are embedded in, or eroded from, technical systems. The political economy of standardisation thus inherently redistributes authority and contributes to regulatory architectures in which public power is exercised through private and semi-private arrangements that often escape conventional forms of democratic control.[2]

2 Understanding the EU's position in the global governance of AI requires more than an institutional or doctrinal reading of the AI Act.[3] It calls for an

* Professor of IT Law (University of Tartu), Research fellow (Florence School of Transnational Governance, EUI

1 Peter Cihon, 'Standards for AI Governance: International Standards to Enable Global Coordination in AI Research & Development' (2019) Future of Humanity Institute Technical Report.

2 Tim Büthe, 'Private Regulation in the Global Economy: A (P)Review' (2010) 12 Business and Politics 1.I introduce a conceptual model \"beyond supply and demand,\" which distinguishes three major subsets of stakeholders of global private regulation, which may (but need not

3 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)[2024] OJ L 12.7.2024.

examination of how value-laden regulatory choices, such as fairness, explainability or bias auditing, are increasingly outsourced to technical standard-setting bodies, many of which are private and structurally insulated from democratic oversight.[4] While the growing role of standards in EU law has been widely recognised, debates have largely concentrated on the legitimacy and accountability of delegating core political functions to non-state actors.[5] Less attention has been paid to the deeper implications of standardisation as a tool of geopolitical influence, or to the ways in which the AI Act could redesign the EU's larger ambition of strategic autonomy in a broader contest over the rules, infrastructures and markets that define the fault lines of AI governance.[6]

3 The interplay between market forces, public authority in the production of AI-related standards stresses the need to re-examine the EU's role and effective influence in shaping regulatory outcomes globally. This concern does not stem from any formal claim by the Union to authority over global standardisation. Rather, it follows from the legal architecture of the AI Act, under which binding obligations relating to risk management, accountability and fundamental rights protection[7] are primarily operationalised through harmonised standards that give rise to a presumption of conformity under Article 40, and whose substantive content is increasingly negotiated in transnational fora. In other words, the practical implementation of the AI Act is dependent on how its legal requirements are translated into technical specifications within international standard-setting processes, thereby making engagement with international standardisation unavoidable rather than optional.[8]

4 In response to this structural dependence, the AI Act adopts a model of conditional openness to international standardisation. Article 40(3) AI Act frames international cooperation on AI standards as permissible only insofar as existing international standards are consistent with Union values, fundamental rights and interests. The same logic is reinforced in the Commission's 2025 standardisation request, which instructs CEN and Cenelec to take into account international ISO and IEC standards while expressly prohibiting reliance on them where compatibility with the purpose, objectives and normative approach of the AI Act cannot be ensured (Recital 16). Arguably, this conditional framework positions standardisation as a site of "selective alignment" through which the Union seeks to preserve regulatory coherence in a fragmented standardisation landscape.

5 The significance of this model of selective alignment becomes clearer when situated within the broader geopolitical context in which AI-related standardisation is taking place. Standard-setting processes in the field of AI are increasingly shaped by competing regulatory models, asymmetric economic power and strategic efforts by states and firms to influence the technical infrastructures that underpin emerging AI markets. In this setting, standards operate as sites of geopolitical contestation that decide whose regulatory preferences become embedded in globally circulating technical norms.

6 At the same time, although formally a piece of internal market legislation under Article 114 TFEU, the AI Act implicitly aspires to shape the global governance of AI by embedding EU political values into technical requirements. By conditioning access to the Union market on compliance with technical requirements that operationalise risk governance, accountability and fundamental rights protection, the Regulation projects its regulatory logic through transnational standardisation processes. Instead of asserting extraterritorial authority directly, the EU

4 Margot Kaminski, 'Voices In, Voices Out: Impacted Stakeholders and the Governance of AI' (*UCLA Law Review*, 21 May 2024) <https://www.uclalawreview.org/voices-in-voices-out-impacted-stakeholders-and-the-governance-of-ai/> accessed 1 September 2025; Charlotte Högberg, 'Stabilizing Translucencies: Governing AI Transparency by Standardization' (2024) 11 Big Data & Society 20539517241234298.21 May 2024

5 Mariolina Eliantonio and Caroline Cauffman, *The Legitimacy of Standardisation as a Regulatory Technique in the EU – A Cross-Disciplinary and Multi-Level Analysis: An Introduction* (Mariolina Eliantonio and Caroline Cauffman eds, Edward Elgar Publishing 2020); Raymund Werle and Eric J Eversen, 'Promoting Legitimacy in Technical Standardization' (2006) 2 Science, Technology & Innovation Studies 19.Edward Elgar Publishing 2020

6 Charlotte Siegmann and Markus Anderljung, 'The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market' (Centre for the Governance of AI 2022); Daniel Mügge, 'EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?' (2024) 31 Journal of European Public Policy 2200; Knut Blind, 'Standardization and Standards: Safeguards of Technological Sovereignty?' (2025) 210 Technological Forecasting and Social Change 123873.\\uc0\\u8216{}EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?\\uc0\\u8217{} (2024

7 See Articles 9-15, 17 and 40 of Regulation (EU) 2024/1689; Commission Implementing Decision C(2025) 3871, recitals (10), (15) and (16).

8 See Articles 40(1) and (3) AI Act; Articles 1(2), 3(1), 6 and 10 Regulation (EU) No 1025/2012. European standardisation is structurally embedded in international standard-setting through cooperation frameworks between CEN and ISO and between Cenelec and IEC, notably under the Vienna Agreement and the Frankfurt Agreement, which operationalise the international cooperation mandate set out in Article 6 Regulation 1025/2012.

relies on internal market law and tools as vehicles for shaping the technical and institutional environments in which AI systems are developed and deployed. This normative ambition reflects the Union's constitutional commitments under Article 16 TFEU, which arguably frames the Act's legal basis within a broader project of value-based digital sovereignty.[9] Such dynamic resonates with accounts of the Brussels Effect. However, the use of standardisation in the AI Act complicates this interpretation. The EU's capacity to shape global regulatory outcomes through standardisation cannot be assumed since it depends on how its normative preferences are translated, negotiated and potentially contested within transnational technical fora.

7 All of the above raises a broader question about the role of standardisation in contemporary regulatory governance. Thus, rather than asking whether the AI Act succeeds or fails on its own terms, this article examines how the EU's reliance on transnational standardisation as a regulatory technique reconfigures authority and power in AI governance, and what this implies for the Union's capacity to shape regulatory outcomes in a geopolitically contested environment. The paper starts from the assumption that the governance of AI through standards is a complex interplay of political, economic and normative forces, where the EU's ability to shape global AI regulation is challenged by geopolitical tensions and the influence of non-EU actors. The paper examines the legal design of the AI Act's delegation to standardisation and the trade-offs embedded in procedural consensus within the wider political economy of technocratic governance. It situates the AI Act's reliance on standardisation in a comparative geopolitical perspective, contrasting the EU's value-oriented model the more market-driven and state-centric approaches associated with the United States and China. The analysis treats the AI Act's standardisation framework as a legal-institutional construct and as a site of (geo)political compromise. In doing so, it examines how delegation to standards development organisations (SDOs) operates as both a necessary functional respond to the complexity and pace of AI development.

8 The paper finds that the EU approach is inherently fragile, as it relies on standards produced by international SDOs[10] over which the EU might not always exercise direct control. The research suggests that consensus in these bodies often masks deep normative and strategic fractures, which may result in advantages for actors with the resources and incentives to dilute or remove concrete safeguards, such as enforceable thresholds for bias testing or requirements for independent reviews, in the name of reaching common agreements. The paper thus emphasises the insufficient normative compatibility between the need to solve a collective action problem and the actual goals of those who produce the standards, and argues that consensus is not (normative) convergence. The paper ultimately questions whether international standards can address the collective action problems of AI and how the EU can effectively navigate these challenges while maintaining its global influence. In so doing, the paper joins a growing branch of the literature expressing misgivings towards the global influence of the AI Act.[11]

9 The paper is structured as follows. It starts by recalling the relevance of standardisation as a site where technical and geopolitical logics overlap. Section 3 examines the EU's strategic role in AI regulation, situating the AI Act within the broader dynamics of global digital governance and its reliance on technical standardisation. Section 4 analyses the political economy of AI-related standardisation and includes some examples on facial recognition, explainability, risk management, bias and fairness auditing, and that show instances of normative divergence in standardisation in these areas. Section 5 places the EU's approach in comparative perspective and presents different futures for the AI Act due to standardisation dynamics. Section 6 concludes by evaluating the EU's prospects for sustaining regulatory influence in AI governance.

B. Taking Standards Seriously

10 In 2003, China revealed a policy introducing the WLAN Authentication and Privacy Infrastructure (WAPI), a domestic wireless encryption protocol that the country sought to establish as a national standard for Wi-Fi-enabled devices. Following this standard was necessary to access the Chinese market. The initiative attracted international attention, not only because of its technical divergence from the globally accepted IEEE 802.11i standard, but also because of

9 Edoardo Celeste, 'Digital Constitutionalism, EU Digital Sovereignty Ambitions and the Role of the European Declaration on Digital Rights' in Annegret Engel, Xavier Groussot and Gunnar Thor Petursson (eds), *New Directions in Digitalisation: Perspectives from EU Competition Law and the Charter of Fundamental Rights* (Springer Nature Switzerland 2025).

10 Annalisa Volpato, Mariolina Eliantonio and Sabrina Röttger-Wirtz (eds), 'Global Standards and EU Law: Introduction' *Global Standards and EU Law* (Edward Elgar Publishing 2025).

11 Robert Mahari and Gabriele Mazzini, 'Sentencing the Brussels Effect: The Limits of the EU's AI Rulebook' (*Social Science Research Network*, 19 June 2025) <https://papers.ssrn.com/abstract=5312437> accessed 14 August 2025; Marco Almada, 'The EU AI Act in a Global Perspective' (*Social Science Research Network*, 17 June 2025) <https://papers.ssrn.com/abstract=5083993> accessed 14 August 2025.

its implications for supply chain dependencies and, ultimately, global regulatory cooperation. At the core of the debate was the extent to which technical standards could be employed to pursue broader industrial and strategic goals.[12]

11 The WAPI episode took place as part of China's wider strategy to reduce reliance on foreign technologies and to strengthen the position of domestic firms in critical digital infrastructure.[13] The protocol's licensing was limited to a selected group of Chinese companies, a move that foreign industry stakeholders viewed with concern.[14] Resistance culminated in an international dispute within the International Organization for Standardization (ISO), where China sought formal recognition of WAPI as an international standard. That attempt was unsuccessful and, in 2006, ISO endorsed the IEEE 802.11i instead. In 2011, after another submission to ISO, the request was eventually withdrawn due to the prolonged inability to find an agreement that would endorse WAPI as a standard by the major international standardisation forum.

12 The WAPI case has often been cited as an early illustration of the strategic use of standardisation in the digital domain.[15] It shows how technical specifications can be entangled with questions of geopolitical power, technological governance and the strategic organisation of digital infrastructures.[16] Rather than serving merely as solutions to coordination problems, standards in such contexts are increasingly framed as instruments of technological autonomy and geopolitical positioning.[17]

13 Standard-essential patents (SEPs) are also an important piece in this regulatory puzzle. By definition, a SEP covers technology that is *essential* for implementing a standard. Thus, any firm wishing to manufacture products compatible with that standard must obtain a licence. As such, SEPs confer a gatekeeping function over entire markets. This confers economic and legal power not only upon patent holders but also upon the institutional frameworks that govern licensing and dispute resolution.[18] Hence, governments are increasingly concerned not only with who holds SEPs but with who participates in the standard-setting processes that give rise to them. Participation in strategic forums, such as 3GPP, ETSI or ISO, has become a form of geopolitical leverage, enabling states to influence technical roadmaps, shape licensing regimes and to project jurisdictional preferences into global regulatory infrastructures.[19]A well-documented example is the growing involvement of Chinese firms in 5G standardisation.[20] Companies

12 Monique Taylor, 'China's Digital Authoritarianism Goes Global' in Monique Taylor (ed), *China's Digital Authoritarianism: A Governance Perspective* (Springer International Publishing 2022); Wenting Cheng, 'China Emerges in International Standardisation' in Wenting Cheng (ed), *China in Global Governance of Intellectual Property: Implications for Global Distributive Justice* (Springer International Publishing 2023).

13 RJEH Creemers, D Broeders and B van den Berg, *China's Conception of Cyber Sovereignty: Rhetoric and Realization* (Rowman & Littlefield 2020); Anne Neuberger, 'China Is Winning the Cyberwar' (*Foreign Affairs*, 13 August 2025) <https://www.foreignaffairs.com/china/china-winning-cyberwar> accessed 13 August 2025.

14 Taylor (n 12).

15 Heejin Lee and Sangjo Oh, 'The Political Economy of Standards Setting by Newcomers: China's WAPI and South Korea's WIPI' (2008) 32 Telecommunications Policy 662; Mi-jin Kim, Heejin Lee and Jooyoung Kwak, 'The Changing Patterns of China's International Standardization in ICT under Techno-Nationalism: A Reflection through 5G Standardization' (2020) 54 International Journal of Information Management 102145; Richard P Suttmeier, 'A New Technonationalism? China and the Development of Technical Standards' (2005) 48 Commun. ACM 35.China attempted to set its national standard for mobile security (wireless LAN authentication and privacy infrastructure (WAPI

16 JoAnne Yates and Craig N Murphy, *Engineering Rules: Global Standard Setting since 1880* (Johns Hopkins University Press 2021); Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (MIT Press 2009).

17 Nicholas Zúñiga and others, 'The Geopolitics of Technology Standards: Historical Context for US, EU and Chinese Approaches' (2024) 100 International Affairs 1635; Tim Rühlig, 'The New Geopolitics of Technical Standardisation: A European Perspective' (2023) 3 Future Europe 102; Marta Cantero Gamito, 'The Influence of China in AI Governance through Standardisation' (2023) 47 Telecommunications Policy 102673.\\uc0\\u8216{}The New Geopolitics of Technical Standardisation: A European Perspective\\uc0\\u8217{} (2023

18 Jorge L Contreras, 'Fixing Frand: A Pseudo-Pool Approach to Standards-Based Patent Licensing' (2013) 79 Antitrust Law Journal 47; Bowman Heiden and Justus Baron, 'A Policy Governance Framework for SEP Licensing: Assessing Private Versus Public Market Interventions' (Social Science Research Network, 23 June 2021) <https://papers.ssrn.com/abstract=3872493>.\\uc0\\u8216{}A Policy Governance Framework for SEP Licensing: Assessing Private Versus Public Market Interventions\\uc0\\u8217{} (Social Science Research Network, 23 June 2021

19 Jorge L Contreras, 'A Research Agenda for Standards-Essential Patents' in Enrico Bonadio and Noam Shemtov (eds), *A Research Agenda for Patent Law* (2025).

20 Riccardo Nanni, 'The "China" Question in Mobile Internet Standard-Making: Insights from Expert Interviews' (2021) 45 Telecommunications Policy 102151; Kim, Lee and Kwak (n 1); Dieter Ernst, 'China's Standard-Essential Patents Challenge: From Latecomer to (Almost) Equal Player? - Centre for International Governance Innovation' (Centre for International Governance Innovation 2017) <https://www.

such as Huawei and ZTE have invested heavily in R&D and now rank among the top holders of SEPs for 5G technologies. This has led to an increasing scrutiny from Western regulators, who view control over 5G SEPs as strategically significant.[21] The European Commission, for instance, has raised concerns about asymmetric SEP licensing practices and launched consultations on the competitiveness and governance of SEP markets.[22] The result is a growing tension between the openness traditionally associated with standardisation (e.g. interoperability, global convergence and diffusion) and the logic of contemporary sovereignty, which privileges strategic sovereignty, control and industrial policy over territoriality and state authority.[23]

14 In view of this, control over SEP governance is increasingly seen as a determinant of Europe's competitiveness in digital markets. The perceived imbalance between jurisdictions that dominate standard-setting and those that merely adopt standards has sparked renewed interest in institutional design, participation incentives and dispute resolution architectures in standardisation.[24]

The geopolitical dimension is also reflected in litigation patterns. Courts have become *de facto* global regulators in SEP licensing disputes, particularly in high-profile cases involving multinational firms. Strategic forum shopping enables patent holders and implementers to seek venues more favourable to their interests, which creates concerns about legal fragmentation and regulatory inconsistency.[25] The *Unwired Planet v. Huawei* case in the UK, for example, marked a significant development when the UK Supreme Court upheld jurisdiction to set global FRAND licensing terms.[26] This is an example of how national courts, in asserting jurisdiction over global licensing disputes, have effectively become instruments for supporting "national champions" or advancing broader industrial policy goals.[27]

15 Hence, regulatory competition is emerging not only between firms but between jurisdictions. China's growing involvement in SEP-intensive sectors has been accompanied by increased state engagement in licensing governance. This includes attempts to reshape the interpretation of FRAND (fair, reasonable, and non-discriminatory) commitments and to advance local firms' positions within standardisation consortia.[28] The EU, the US, and other actors are responding in turn, proposing new rules for SEP transparency, licensing terms and dispute resolution mechanisms. For instance, although recently withdrawn, the EU's draft regulation on SEPs reflects this broader shift, positioning SEP governance as a lever of digital sovereignty.[29]

16 The implications of these developments are significant. The value of participating in standard-setting is thus not limited to shaping technology. It also extends to influencing the conditions under which legal certainty, market access and competitive advantage are distributed. Given the relevance of standards in defining digital governance, the role of courts, regulatory authorities and standard-setting organisations requires continuous scrutiny as actors

cigionline.org/publications/chinas-standard-essential-patents-challenge-latecomer-almost-equal-player/>."plain Citation":"Riccardo Nanni, 'The "China" Question in Mobile Internet Standard-Making: Insights from Expert Interviews' (2021

21 Carolyn Bartholomew, 'China and 5g' (2020) 36 Issues in Science and Technology 50; Jiabao Sun and Zhanpeng Wang, 'Huawei 5G in the UK: (De)Politicisation, Geopolitics and Expertise' (2024) 19 British Politics 106.

22 European Commission (2023). Proposal for a Regulation on Standard Essential Patents. COM(2023) 232 final.

23 John Agnew, 'Sovereignty Regimes: Territoriality and State Authority in Contemporary World Politics' (2005) 95 Annals of the Association of American Geographers 437.drawing from recent research in political geography and other fields, are that sovereignty is neither inherently territorial nor is it exclusively organized on a state-by-state basis. This matters because so much political energy has been invested in organizing politics in general and democracy in particular in relation to states. Typically, writing about sovereignty regards sovereignty as providing a norm that legitimizes central state authority. Unfortunately, little or no attention is given as to why this should always entail a territorial definition of political authority and to why states are thereby its sole proprietors. The dominant approach continues to privilege the state as the singular font of authority even when a state's sovereignty may be decried as hypocrisy and seen as divisible or issue-specific rather than "real" or absolute. I put forward a model of sovereignty alternative to the dominant one by identifying four "sovereignty regimes" that result from distinctive combinations of central state authority (legitimate despotic power

24 Armelle Mazé, 'Standard-Setting Activities and New Institutional Economics' (2017) 13 Journal of Institutional Economics 599.

25 Garry Gabison, 'Worldwide FRAND Licensing Standard' (2019) 8 American University Business Law Review 139.

26 UKSC/2018/0214.

27 Jorge L Contreras and Martin Husovec, 'Issuing and Tailoring Patent Injunctions: A Cross-Jurisdictional Comparison and Synthesis' in Jorge L Contreras and Martin Husovec (eds), *Injunctions in Patent Law: Trans-Atlantic Dialogues on Flexibility and Tailoring* (Cambridge University Press 2022).

28 Zhang Yu and Zhong Chun, 'Decoding China's SEP Antitrust Guidelines: Key Provisions, Challenges, and EU Comparisons' (2025) 16 Journal of European Competition Law & Practice 314.

29 Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (European Commission) and others, *Empirical Assessment of Potential Challenges in SEP Licensing* (Publications Office of the European Union 2023).

in a changing global order. The following section addresses the AI Act's approach to standardisation in this geopolitical perspective.

C. Why Standards? The Strategic Logic Behind the EU's Regulatory Choice

I. From the New Legislative Framework to the AI Act

17 The EU's choice to rely on technical standardisation as the central mechanism for operationalising the AI Act is neither arbitrary nor unprecedented. It reflects a deeply embedded legal-institutional logic rooted in the New Legislative Framework (NLF), which has structured EU product regulation since 2008.[30] The NLF builds on the "New Approach" to technical harmonisation and standards, first introduced in 1985.[31] Under this model, legislation defines essential requirements, often formulated in high-level, generic terms, while harmonised standards developed by the recognised European Standardisation Organisations ('ESOs'; CEN, CENELEC and ETSI) provide the concrete specifications necessary to demonstrate compliance. Once these standards are cited in the Official Journal of the European Union and assessed for suitability, they create a legal **presumption of conformity** with the relevant legislative obligations. The AI Act imports and adapts this architecture. Article 40 establishes the foundational role of harmonised standards for demonstrating compliance with the core legal requirements of the Regulation. For general-purpose AI models ('GPAI'), the Act provides that codes of practice may serve this function upon formal recognition by the European Commission.[32] While harmonised standards are, in principle, voluntary, their role in determining access to the EU market and their function in enabling conformity assessments renders them *de facto* **binding**.[33]

18 A growing body of interdisciplinary scholarship has challenged the long-standing assumption that technical standards are neutral instruments of technical coordination, and showed how standardisation constitutes a site where power, expertise and normative authority intersect.[34] While standards often emerge through procedures that frame them as the output of expert-driven technocratic deliberation, their effects reach far beyond technical implementation. They translate vague legal principles into concrete obligations and, as such, standards design the architecture of legal obligations in ways that may be neither transparent nor politically neutral.[35]

19 This conceptual shift has invited a closer examination of the institutional structures and decision-making processes through which standards are developed. Standard-setting bodies operate in a hybrid legal space that blends public interest functions with private governance mechanisms.[36] Their decisions increasingly acquire normative force, especially in domains where adherence to a given standard determines market access or legal conformity.[37] In AI-related standardisation, standards translate broad legal concepts such as 'safety', 'trustworthiness' or 'human oversight' into operational benchmarks. Thus, standards resolve legal ambiguity and bridge the gap between abstraction and operational requirements. Yet this process of translation is rarely insulated from value judgment. The specification of what counts as acceptable risk, sufficient transparency or robust mitigation measures is deeply shaped by the epistemologies, interests and even the very own resources of the actors involved in standard development.[38] In practice, this means

30 Sybe de Vries, Olia Kanevskaia and Rik de Jager, 'Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation' (2023) 2023 8 European Papers - A Journal on Law and Integration 583610.

31 European Commission, Technical Harmonization and Standards: A New Approach to COM. (85) 19 final. Brussels 31 January 1985.

32 Article 53(4).

33 C-171/11, *Fra.bo*, EU:C:2012:453, paras 29 and 30. See also Harm Schepel, 'The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law' (2013) 20 Maastricht Journal of European and Comparative Law 521; Marta Cantero Gamito and Christopher T Marsden, 'Artificial Intelligence Co-Regulation? The Role of Standards in the EU AI Act' (2024) 32 International journal of law and information technology.

34 Langdon Winner, 'Do Artifacts Have Politics?' (1980) 109 Daedalus 177; Tim Büthe, 'Global Private Politics: A Research Agenda' (2010) 12 Business and Politics; Laura DeNardis, 'Hidden Levers of Internet Control' (2012) 15 Information, Comunication & Society 720; Harm Schepel, *The Constitution of Private Governance : Product Standards in the Regulation of Integrating Markets* (Hart Publishing 2005).

35 Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011); Sandra Lavenex, Omar Serrano and Tim Büthe, 'Power Transitions and the Rise of the Regulatory State: Global Market Governance in Flux' (2021) 15 Regulation and Governance 445; Kenneth W Abbott and others, *International Organizations as Orchestrators* (Kenneth W Abbott and others eds, Cambridge University Press 2015).

36 Schepel (n 9); On a more recent account in EU digital policy, see Annalisa Volpato, 'The Publicity of EU Law and the Privatization of EU Digital Regulation' (2024) 31 Maastricht Journal of European and Comparative Law 319.

37 Eliantonio and Cauffman (n 5).

38 Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act —

that standards perform a critical function as they set the legal and technical conditions under which compliance is assessed.

20 Furthermore, the notion that standardisation is merely a form of soft law has thus become increasingly difficult to sustain. As legal instruments, standards may not always be binding in the formal sense, but their integration into regulatory frameworks and conformity assessment schemes gives them a quasi-legislative effect.[39] This blurred boundary between soft coordination and hard compliance has led scholars to describe standardisation as a form of transnational rulemaking that escapes traditional legal classifications.[40]

21 From a legal-institutional perspective, this model raises fundamental questions about legitimacy. The legal literature has long highlighted the tension between the flexibility offered by standardisation and the need for public oversight when such instruments acquire binding legal effect.[41] This tension is amplified in the digital domain, where the normative content of standards increasingly shapes rights, obligations and enforcement structures in ways that are difficult to contest or even access.[42] One of the most visible manifestations of this problem is the **copyright status of technical standards**. Standards incorporated by reference into EU law are often not freely available to the public, which raises concerns about legal certainty and accessibility of the law. This issue has recently come before the Court of Justice of the European Union, where the Court examined the accessibility of paywalled harmonised standards when referenced in EU legislation.[43] The Court overturned the General Court's judgment and recognised that, owing to their legal effects and their role in determining rights and obligations, harmonised standards form part of EU law.[44] As such, the Court held that access to these standards is justified under the principle of the rule of law and the overarching principles of legal certainty and transparency.[45] The ruling aligns with earlier doctrinal positions taken by the Court. In *Fra.bo*, the Court noted that while alternative compliance pathways are in theory available, they may be practically unfeasible due to administrative burdens and cost, thus reinforcing the quasi-obligatory nature of harmonised standards.[46] Here, the Court extended the application of EU fundamental freedoms to private certification bodies, holding that non-State actors involved in essential regulatory functions may fall under EU law scrutiny. Similarly, in *James Elliott Construction*, the Court held that harmonised standards, once published in the Official Journal, form part of EU law due to their legal effects, particularly the presumption of conformity.[47] The Court thus complemented the previous interpretation given in *Stichting*, where it reaffirmed that (ISO) standards may bind the public where their legal effects are conferred by EU law.[48] Accordingly, the case law thus recalibrates the balance between intellectual property protection and public access, and while acknowledging that harmonised standards are developed by private organisations and retain copyright protection, the Court prioritised the public's ability to ascertain their rights and obligations under EU law.

22 Despite the case law and the AI Act's commitment to inclusiveness and multistakeholder participation Article 40(3) does not alter the structural reality of **industry-dominated standard-setting**. As noted in the literature, the production of AI-related standards remains largely controlled by corporate actors with the resources to engage in technical, and somehow arcane, standardisation processes.[49] To date, civil society, SMEs and public-interest groups still face structural barriers to participation, from limited access to expert knowledge to procedural opacity

Analysing the Good, the Bad, and the Unclear Elements of the Proposed Approach' (2021) 22 Computer Law Review International 97.

39 Harm Schepel, 'The New Approach to the New Approach: The Juridification of Harmonized Standards in EU Law' (2013) 20 Maastricht Journal of European and Comparative Law 521; Hans-W Micklitz, 'Chapter 10: Soft Law, Technical Standards and European Private Law' in Mariolina Eliantonio, Emilia Korkea-Aho and Ulrika Mörth (eds), *Research Handbook on Soft Law* (Edward Elgar Publishing 2023).

40 Nils Brunsson and Bengt Jacobsson, *A World of Standards* (Nils Brunsson and Bengt Jacobsson eds, Oxford University Press 2002); Fabrizio Cafaggi, 'New Foundations of Transnational Private Regulation' (2011) 38 Journal of Law and Society 20.

41 Eliantonio and Cauffman (n 5); Deirdre Curtin and Linda Senden, 'Public Accountability of Transnational Private Regulation: Chimera or Reality' (2011) 38 Journal of Law and Society 163; Colin Scott, Fabrizio Cafaggi and Lisa Senden, 'The Conceptual and Constitutional Challenge of Transnational Private Regulation on JSTOR' (2011) 38 Journal of Law and Society 1.

42 Hans-W Micklitz, 'The Role of Standards in Future EU Digital Policy Legislation. A Consumer Perspective' (ANEC and BEUC 2023); Volpato (n 36).

43 Case C-588/21 P - *Public.Resource.Org and Right to Know v Commission and Others*. ECLI:EU:C:2024:201.

44 Ibid. Para 70.

45 See para 81.

46 C-171/11 - *Fra.bo*. ECLI:EU:C:2012:453.

47 C-613/14 - *James Elliott Construction Limited v Irish Asphalt Limited*. ECLI:EU:C:2016:821.

48 C-160/20 - *Stichting Rookpreventie Jeugd and Others*. ECLI:EU:C:2022:101. And more recently, C-155/24 - *Stichting II*. ECLI:EU:C:2026:327

49 Marco Almada and Nicolas Petit, 'The EU AI Act: Between the Rock of Product Safety and the Hard Place of Fundamental Rights' (2025) 62 Common Market Law Review; Cantero Gamito and Marsden (n 33).

within standard-setting organisations.[50] This raises concerns not only of epistemic asymmetry but also of **democratic legitimacy in AI governance**, particularly when standards are to shape obligations for transparency or algorithmic accountability, which ultimately impact fundamental rights.[51]

23 Considering these concerns, the European legislator has foreseen some guarantees to oversee the delegation process. For example, the AI Board is intended to provide some degree of public oversight of this process by assessing whether harmonised standards or codes of practice are suitable to satisfy the legal requirements of the AI Act.[52] Yet the nature and depth of this oversight function remain ambiguous and only time will tell the extent and effectiveness of it. Moreover, as the literature has argued in the context of EU agencies more broadly, formal review powers do not guarantee substantive scrutiny.[53] Therefore, if the AI Board lacks adequate independence, expertise or procedural precision the delegation to standard-setting risks becoming a **procedural rubber stamp** for private norm production. In this regard, it is important to consider Article 41, which introduces the possibility for the European Commission to adopt **'common specifications'** when harmonised standards or codes of practice are unavailable or insufficient. However, although this regulatory choice offers a safeguard to "reinsert" public regulatory authority into this scheme, it also introduces complexity because the coexistence of multiple normative instruments (standards, codes, commons specifications) may create potential for overlap and legal fragmentation.

24 More broadly, this delegation model reconfigures the legal landscape of digital regulation.[54] Arguably, the AI Act risks becoming a form of **proprietary regulation,** in which market access is mediated by quasi-private norms and compliance costs are absorbed asymmetrically across the digital ecosystem.[55] This has profound implications for market structure, competition and innovation, as this approach seemingly favours actors that can internalise the costs of standardised compliance and contribute to the shaping of the standards themselves.[56] In this sense, the AI Act risks giving rise to a form of *de facto* private regulatory influence, whereby firms that possess the resources to participate in standard-setting, absorb the costs of compliance engineering and shape technical specifications are better positioned both to meet regulatory requirements and to influence how those requirements are operationalised. This dynamic has implications for market structure, competition and innovation, as it may favour large or incumbent, i.e. non-EU, actors capable of internalising compliance costs and contributing to standard design, while disadvantaging smaller firms and new entrants that must comply with standards they had little role in shaping.

25 Still, the problem is not merely that there is delegation to private actors, but that there are a set of concerns the debilitate the current institutional design of this delegation. Delegation to decentralised standard-setting bodies can enhance epistemic robustness and administrative scalability in highly complex and rapidly evolving technological domains and has long been a constitutive feature of EU internal market governance.[57] The difficulty arises, however, from the specific institutional design through which delegation under the AI Act is structured, and the conditions under which it operates. Where harmonised standards serve to operationalise normatively dense legal obligations, the reliance on consensus-based standard-setting in transnational fora exposes the regulatory framework to pressures that EU law is only partially equipped to discipline.[58]

26 This vulnerability is intensified by the geopolitical context of AI-related standardisation and by the AI Act's reliance on common specifications as a fallback mechanism. The solution found in common specifications formally conceived as an instrument to preserve legal certainty where harmonised standards are delayed, contested or absent, also reveal the limits of decentralised governance in the face of normative disagreement and strategic contestation.[59] In practice, the availability of common

50 Justus Baron and Pierre Larouche, The European Standardisation System at a Crossroads (Centre on Regulation in Europe (CERRE) 2023) https://cerre.eu/publications/the-european-standardisation-system-at-a-crossroads/ accessed 2 September 2025.

51 Almada and Petit (n 49); Cantero Gamito and Marsden (n 33); Veale and Borgesius (n 38).serif\"><i>The European Union (EU

52 Article 66 let e).

53 R Daniel Kelemen, *Eurolegalism: The Transformation of Law and Regulation in the European Union* (Harvard University Press 2011); Deirdre Curtin and Morten Egeberg, 'Tradition and Innovation: Europe's Accumulated Executive Order' (2008) 31 West European Politics 639.

54 Volpato (n 36); Micklitz (n 42); de Vries, Kanevskaia and de Jager (n 30).

55 Cantero Gamito and Marsden (n 33).

56 Ibid.

57 Giandomenico Majone (ed), *Regulating Europe* (Routledge 2002); Marise Cremona, 'The Union as a Global Actor: Roles, Models and Identity' (2004) 41 Common Market Law Review; Schepel (n 33)."plainCitation":"Giandomenico Majone (ed

58 Christian Joerges, '"Deliberative Supranationalism"—Two Defences' (2002) 8 European Law Journal 133.

59 Marta Cantero Gamito, 'From Consensus to Exceptionality – What the EU's AI Standards Crisis Reveals About Delegated Technical Governance, by Marta Cantero Gamito' (*REALaw.*

specifications does not eliminate power asymmetries within standard-setting processes, but may instead reshape incentives within them, reinforcing the position of actors capable of influencing both the content of standards and subsequent regulatory interventions.[60] Under these conditions, delegation operates within an environment characterised by asymmetric resources, strategic coordination and external political pressure, in which consensus may obscure rather than resolve normative divergence.

27 Accordingly, the AI Act's legal-institutional infrastructure cannot be analysed in isolation from its geopolitical context. As discussed in subsequent sections, its reliance on standardisation must be understood as part of a broader strategic agenda to shape the global governance of AI through infrastructural rather than extraterritorial means. Standards are thus not only instruments of internal regulatory efficiency but also tools of external **normative projection** that embeds EU priorities in global markets, supply chains and compliance architectures.[61]

II. The Strategic Appeal of Standards

28 Despite the concerns outlined above, it can be said that standardisation has become the EU's preferred mechanism for implementing AI regulation, and not merely for reasons of legal efficiency but as an instrument of geopolitical strategy.[62] The delegation to standards may enable the EU to future-proof its regulatory regime and project normative power globally without the legal or diplomatic costs of extraterritorial legislation.[63] There are several reasons supporting this regulatory strategy.

29 First, standards provide the flexibility that formal legislation lacks. Unlike hard law, which requires consensus and often becomes outdated by the time it is enacted, standards can be continuously updated to reflect technological developments.[64] This is crucial in the regulation of AI, where innovation outpaces institutional response and legal certainty must coexist with technical adaptability. This delegation to standard-setting under the AI Act can ensure that the Regulation remains formally neutral, while standards supply the necessary normative specificity. The resulting regulatory structure facilitates fast adaptation to evolving risks and market conditions without reopening political debate.[65]

30 Second, the reliance on standards is also a mechanism of industrial policy. The AI Act reliance on conformity assessment, technical documentation and post-market monitoring can, in practice, create quasi-barriers to entry by redistributing compliance burdens in ways that stabilise Europe's industrial base and service infrastructure.[66] Notified bodies and consultancy firms gain a central role in implementing the AI Act, which means transforming standard compliance into a legally constructed source of economic advantage rooted in credentialed expertise, regulatory gatekeeping and mandatory conformity assessment processes.[67] The AI Act can thus function as an instrument that can contribute to Europe's capacity to shape the AI value chain in accordance with its institutional and economic configurations.[68]

blog, 28 November 2025) <https://realaw.blog/2025/11/28/from-consensus-to-exceptionality-what-the-eus-ai-standards-crisis-reveals-about-delegated-technical-governance-by-marta-cantero-gamito/> accessed 30 January 2026.

60 Nigel Cory, 'How the EU Is Using Technology Standards as a Protectionist Tool In Its Quest for Cybersovereignty' (*Information Technology & Innovation* Foundation, 19 September 2022) <https://itif.org/publications/2022/09/19/how-the-eu-is-using-technology-standards-as-a-protectionist-tool/> accessed 4 August 2025; Nigel Cory, 'Europe Goes Protectionist on Global Technical Standards: The Example of "Common Specifications' (*Information Technology & Innovation* Foundation, 24 February2023) <https://itif.org/publications/2023/02/24/europe-goes-protectionist-on-global-technical-standards-the-example-of-common-specifications/> accessed 4 August 2025.

61 See Marta Cantero Gamito and Hans Micklitz, *The Role of the EU in Transnational Legal Ordering: Standards, Contracts and Codes* (Edward Elgar Publishing 2020).

62 Alessandro Mantelero, 'The AI ACT: A Geopolitical Tool to Foster Human Rights and Ethics' in Diego Brasioli and others (eds), *Routledge Handbook of Artificial Intelligence and Geopolitics* (Routledge 2025).artificial intelligence (AI

63 Joanne Scott, 'The New EU "Extraterritoriality"' (2014) 51 Common Market Law Review <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\COLA\COLA2014110.pdf> accessed 13 August 2025; Cantero Gamito and Micklitz (n 61).

64 Mike Teodorescu and Makridis Christos, 'Fairness in Machine Learning: Regulation or Standards?' (*Brookings,* 15 February 2024) <https://www.brookings.edu/articles/fairness-in-machine-learning-regulation-or-standards/> accessed 4 August 2025.

65 Cary Coglianese and Colton R Crum, 'Regulating Multifunctionality' (*arXiv*, 26 January 2025) <http://arxiv.org/abs/2502.15715> accessed 4 August 2025.

66 Cantero Gamito and Marsden (n 33).

67 Jakob Mökander and others, 'Conformity Assessments and Post-Market Monitoring: A Guide to the Role of Auditing in the Proposed European AI Regulation' (2022) 32 Minds and Machines 241; Eva Thelisson and Himanshu Verma, 'Conformity Assessment under the EU AI Act General Approach' (2024) 4 AI and Ethics 113.\\uc0\\u8216{} Conformity Assessment under the EU AI Act General Approach\\uc0\\u8217{} (2024

68 Raluca Csernatoni, 'The EU's AI Power Play: Between Deregulation and Innovation | Carnegie Endowment for

31 Third, delegating implementation to private standardisation bodies also serves a political function. It allows EU institutions to circumvent politically charged debates around controversial AI uses such as biometric surveillance, emotion recognition or algorithmic biases. Instead, it embeds technical criteria within closed technical processes. This is consistent with what Majone had noted some 30 years ago in relation to EU lawmaking while arguing that technocratic delegation is often used to reduce democratic contestation in a way that normative decisions are reframed as technical ones.[69] The AI Act exemplifies this shift. It frames standardisation as an inclusive and future-oriented tool. Yet, in practice, the development of standards remains dominated by industry actors and shaped by market incentives.[70] This configuration insulates key regulatory decisions from public scrutiny while preserving the appearance of neutral, expert-led governance.

32 And fourth, altogether, standards have become one of the EU's preferred vehicles for global normative projection.[71] This approach is rooted in the strategic insight that infrastructure can serve as a more effective conduit of influence than law. As described above, by shaping the technical conditions for market access, the EU embeds its regulatory choices into global supply chains and conformity regimes. As such, standards function as invisible devices of sovereignty. They govern technical interoperability but also supply chain inclusion or risk certification, with consequences that decide who can participate in the EU digital market and on what terms. Externally, the semi-expansionist inclination is evident in Article 40(3), which speaks of international cooperation in the development and promotion of standards 'that are consistent with Union values, fundamental rights and interests'. Moreover, unlike binding legislation, harmonised standards (and codes of practice, in particular) are less likely to be challenged in WTO dispute settlement proceedings or interpreted as digital imperialism. Some commentators have noticed that this "standards-first" strategy allows the EU to advance a preferential industrial agenda while maintaining plausible deniability under the rhetoric of openness and cooperation.[72] Arguably, the delegation to standards and other co-regulatory instruments (i.e. Codes of practice) in the AI Act blurs the line between purely internal market regulation and external geopolitical strategy, which results in geopolitical ambivalence. It creates a system of market governance that appears open and non-binding but that in practice disciplines access, structures compliance costs and embeds specific normative values.

33 All things considered, the strategic appeal of standards lies in their manifold possibilities. They allow the EU to pursue multiple, often contradictory goals such innovation-friendly regulatory adaptability and normative stability (especially, in a sector marked by fast-paced development), market integration and industrial protectionism, depoliticisation and geopolitical ambition. Seen this way, the turn to standardisation and co-regulation is a choice for regulatory design in which, in addition to tools of compliance, standards can also serve as proxies of strategic influence, domestically and globally.

D. The Geopolitical Economy of AI-related Standardisation

I. Who Sets the Standards?

34 The delegation of regulatory authority to technical standardisation bodies redistributes power across a transnational terrain populated by public institutions, private firms, industrial consortia and international organisations.[73] Provided that AI-related standardisation implies to decide what normative choices are embedded into infrastructure, exploring who sets the standards, and under what conditions, is essential to fully understand the implications of the EU's regulatory strategy.

35 At the international level, the AI standardisation ecosystem is embedded in a set of formal SDOs, most prominently the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers Standards Association (IEEE SA). A central node in this landscape is ISO/IEC JTC 1, and in particular its Subcommittee 42 (SC 42) on Artificial Intelligence,

International Peace' (*Carnegie Endowment for International Peace,* 20 May 2025) < https://carnegieendowment.org/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation> accessed 4 August 2025.

69 Giandomenico Majone, 'The Rise of the Regulatory State in Europe' (1994) 17 West European Politics 77.

70 Almada and Petit (n 49).

71 Anu Bradford, 'Exporting Standards: The Externalization of the EU's Regulatory Power via Markets' (2015) 42 International Review of Law and Economics 158; Cantero Gamito and Micklitz (n 61).

72 Cory, 'How the EU Is Using Technology Standards as a Protectionist Tool In Its Quest for Cybersovereignty' (n 60).

73 Panagiotis Delimatsis, 'Introduction: Continuity and Change in International Standardisation', in *The Law, Economics and Politics of International Standardisation* (Cambridge University Press 2015).

which coordinates work on AI terminology, governance, trustworthiness, computational methods, use cases, and big data. SC 42 interacts with over a dozen liaison organisations, including UN bodies and industry consortia, and works through multiple Working Groups.

36 In the United States, the standardisation system is deliberately decentralised. It relies on a bottom-up, industry-led approach coordinated loosely through the National Institute of Standards and Technology (NIST), which issues voluntary frameworks and guidelines (e.g., the NIST AI Risk Management Framework), but does not itself develop binding technical standards. This model reflects the broader US regulatory philosophy of minimal intervention and embraces the idea that innovation should not be constrained by prematurely rigid norms.[74] As such, it allows major technology firms to dominate standard-setting both at home and abroad, particularly through their strategic engagement in ISO, IEC and IEEE processes.

37 In contrast, China pursues a state-led strategy of standardisation aligned with its broader industrial policy and geopolitical goals. AI standards are developed through national bodies such as the Standardization Administration of China (SAC) and Technical Committee 260 (TC260), which are closely linked to the Ministry of Industry and Information Technology (MIIT) and the Chinese Communist Party. These bodies embed national priorities, including cybersecurity, social stability and surveillance capabilities, directly into the technical content of standards.[75] China also seeks to internationalise its standards by actively participating in ISO and IEC committees, often advocating for terminology, metrics, and conformity procedures that reflect its domestic model of governance. The strategic use of standards in China's AI policy forms part of its "Digital Silk Road" initiative, aimed at embedding Chinese technical norms into the digital infrastructure of the Global South.[76]

38 The EU stands in the middle. It delegates standard-setting to recognised ESOs under a public-private governance model.[77] ESOs operate under the legal framework of Regulation (EU) No 1025/2012 on European Standardisation.[78] As seen above, the EU model is designed to maintain flexibility and technical neutrality but, in practice, it had largely mirrored many of the participation asymmetries seen in global SDOs.[79]

39 This institutional configuration gives rise to three critical observations. First, the representation of interests in AI standardisation is structurally skewed. In all three jurisdictions (US, China, and the EU) private industry plays a central, if differently institutionalised, role in shaping the content of standards. In the US, corporate dominance is explicit and aligned with regulatory *laissez-faire*. In China, state-guided corporatism blends public authority with industrial and commercial goals. In the EU, the delegation model preserves the formal appearance of neutrality and public oversight but embeds corporate influence through procedural and epistemic control.[80]

40 Second, the geopolitical orientation of standardisation strategies varies sharply. While the US sees standards as tools of industrial leadership and market dominance and China as proxies of techno-political sovereignty, the EU frames its strategy as one of regulatory cooperation and normative diffusion. However, the EU's increasing reliance on standards to secure market access and promote its values abroad carries a protectionist undertone.[81] In particular, the adoption of common specifications when harmonised standards fail or are delayed (something to be unilaterally decided by

74 Emily S Bremer, 'American and European Perspectives on Private Standards in Public Law' (*Social Science Research Network*, 1 December 2016) <https://papers.ssrn.com/abstract=2758904> accessed 2 September 2025; Jamal Shahin, 'Dancing to the Same Tune? EU and US Approaches to Standards Setting in the Global Digital Sector' (2024) 46 Journal of European Integration 1111.\\uc0\\u8216{} Dancing to the Same Tune? EU and US Approaches to Standards Setting in the Global Digital Sector\\uc0\\u8217{} (2024

75 Junhua Zhu, *China's Approach to AI Standardisation: State-guided but Enterprise-led* (Briefing Paper 391, Finnish Institute of International Affairs 2024).

76 ibid.

77 Schepel (n 34).

78 Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council Text with EEA relevance. OJ L 316, 14.11.2012, pp. 12–33.

79 Rob van Gestel and Hans-W Micklitz, 'European Integration through Standardization: How Judicial Review Is Breaking down the Club House of Private Standardization Bodies' (2013) 50 Common Market Law Review 145.

80 Linda Senden, 'Chapter 2: Towards a More Holistic Legitimacy Approach to Technical Standardisation in the EU' in Mariolina Eliantonio and Caroline Cauffman (eds), *The Legitimacy of Standardisation as a Regulatory Technique* (Edward Elgar Publishing 2020).

81 Cory, 'Europe Goes Protectionist on Global Technical Standards' (n 60).

the European Commission) is seen as a way of public regulatory control over standardisation but also as a strategic fallback mechanism to shape compliance terms and insulate European preferences from international dilution.[82]

41 And third, AI standardisation operates within a global environment characterised by pronounced structural imbalances, competing normative agendas and a high degree of strategic interdependence.[83] The EU's engagement in this sphere functions both as a response to and a tool for ongoing geopolitical shifts. Positioned between the US and the Chinese models, it seeks to embed its own normative framework into the technical architecture that underpins AI governance. The extent to which this approach can be sustained and the implications it may have for the normative trajectories of AI governance are examined in the following sections.

II. Some Case Studies of Normative Divergence in Standardisation

42 While international standards can propagate best practices globally, their normative governance impact depends crucially on who designs them and with what intention.[84] In this regard, SDOs face structural obstacles in governing frontier AI issues. Despite reputational authority, they struggle to standardise state-of-the-art concerns (e.g. LLM fairness) precisely because technological complexity outpaces institutional capacity.[85] These observations challenge the legitimacy and effectiveness of global consensus-based processes when value-laden divergences appear.

1. Facial Recognition and Transparency Standards

43 The development of facial recognition standards has shown profound divergence in how ethical risks are conceptualised and mitigated with standards. The IEEE's P7000 series (particularly P7001 on transparency and P7013 on algorithmic bias) frames ethics through human-centric values, given its emphasis on consent, oversight and procedural due process. Although IEEE P7001 is not about facial recognition specifically, its general framework for algorithmic transparency is often invoked in this domain to illustrate how high-level ethical principles, such as explainability, interact with sensitive, real-world applications.[86] Yet this generalisation is a double-edged sword because while it promotes broad acceptance, it lacks the sectoral specificity needed to address biometric harms or power asymmetries embedded in surveillance technologies.[87] In this regard, IEEE P7001 has been found to face important challenges. Its definition of transparency is vague, often conflating technical explainability with legal or ethical accountability.[88] Additionally, P7001 does not prescribe enforceable mechanisms and it is liable to being reduced to procedural formalism.[89] As a result, it risks being overly technocratic and disconnected from real-world power asymmetries and fails to clarify to whom, about what and for what purpose transparency is due.[90]

44 The framing of transparency in P7001 can be considered rooted in liberal democratic ideals of individual agency, informed consent and rights-based governance, all of which are characteristics of Western epistemologies that reflect the liberal-individualist tradition dominant in US and EU academic discourse.[91] In contrast, and as a manifestation of its different understanding of AI governance, China's GB/T 41391-2022 standard, developed under SAC/TC260 (the National Technical Committee 260 on Cybersecurity of Standardization Administration of China)[92] prioritises social

82 Ibid.

83 Cantero Gamito (n 17).community- and largely industry-driven processes. Governments are increasingly interested in technical standards' development, accentuating the political dimension of standardisation. This article explores the contribution of technical standardisation to the governance of artificial intelligence (AI

84 Cihon (n 2).

85 Huw Roberts and Marta Ziosi, 'Can We Standardise the Frontier of AI?' (*Social Science Research Network*, 27 May 2025) <https://papers.ssrn.com/abstract=5271446> accessed 1 August 2025.

86 Högberg (n 4).

87 Sebastian Bordt and others, 'Post-Hoc Explanations Fail to Achieve Their Purpose in Adversarial Contexts', *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (Association for Computing Machinery 2022) <https://dl.acm.org/doi/10.1145/3531146.3533153> accessed 1 August 2025.

88 David Schneeberger and others, 'The Tower of Babel in Explainable Artificial Intelligence (XAI)' in Andreas Holzinger and others (eds), *Machine Learning and Knowledge Extraction* (Springer Nature Switzerland 2023).

89 Brady Lund and others, 'Standards, Frameworks, and Legislation for Artificial Intelligence (AI) Transparency' (2025) 5 AI and Ethics 3639.

90 Alan FT Winfield and others, 'IEEE P7001: A Proposed Standard on Transparency' (2021) 8 Front Robot AI 665729 <https://doi.org/10.3389/frobt.2021.665729>.

91 Mike Ananny and Kate Crawford, 'Seeing without Knowing: Limitations of the Transparency Ideal and Its Application to Algorithmic Accountability' (2018) 20 New Media & Society 973.

92 GB/T 41391-2022. Information security technology—Basic requirements for collecting personal information in mobile internet applications, <https://www.codeofchina.com/

stability and with public safety.[93] A closer look at this domestic discourse complicates the picture. As recent studies show, facial recognition technologies have become the subject of intense public debate within China, including complaints and online backlash.[94] However, these frictions rarely translate into standardisation forums such as SAC/TC260, which remain regime-aligned and largely insulated from civil society participation. In this regard, it is precisely the gap between public contestation and technical formalisation what marks a key contrast with the multi-stakeholder ethos underpinning the IEEE P7000 series, even if the latter suffers from implementation imprecision and global legitimacy challenges.[95]

45 Meanwhile, Article 5(1) let d) AI Act establishes a general prohibition on real-time remote biometric identification in public spaces, subject to narrow exceptions (notably for law enforcement in cases of serious crime, search for missing persons, or prevention of imminent threats). However, while framed as a ban, many scholars argue these exceptions weaken the measure to the point that it cannot be regarded as a true "hard line".[96] Despite this significant limitation, this more rights-based approach followed by the EU legislator regarding surveillance signals a normative divergence from both IEEE's voluntary ethics and China's surveillance-oriented technical standards.

2. Explainability

46 The P7000 is just one example of how 'transparency' and 'explainability' are subject to varied interpretations across regions. ISO SC 42 has also dedicated projects to pin down these concepts after having recognised that consensus was initially absent. For example, ISO/IEC AWI 12792 (under publication) proposes a 'transparency taxonomy' to clarify what information elements different AI stakeholders need.[97] Similarly, ISO/IEC TS 6254 (under publication) seeks to describe approaches to explainability and interpretability for machine learning models. These efforts arose because different players attach different meanings and importance to explainability.[98] Despite the standardisation efforts no common vocabulary exists yet.

47 Geopolitics can also explain this divergence. In the EU context, explainability can be understood as a legal requirement under the AI Act. Article 13(1) obliges providers of high-risk AI systems to design and develop them so they are 'sufficiently transparent to enable users to interpret the system's output and use it appropriately'.[99] Article 14 then links explainability to human oversight, requiring that systems be designed to allow natural persons to effectively monitor high-risk AI systems' functioning and correctly interpret the system's output. The Regulation does not prescribe a specific technical approach for explainability. Therefore, the lack of international consensus means that the definition of the operational details by harmonised standards may result in international divergences in terminology or methodology, which will directly affect compliance within the EU.

48 Within this divergence, the EU views explainability/transparency as rights-based (e.g. a 'right to explanation' for individuals and a prerequisite for accountability), reflecting GDPR roots and the AI Act's human-centric approach, even if criticised for impracticable.[100] As seen above, China, by contrast, includes transparency among its AI governance

standard/GBT41391-2022.html>.

93 Yan Luo and Rui Guo, 'Facial Recognition in China: Current Status, Comparative Approach and the Road Ahead' (2021) 25 University of Pennsylvania Journal of Law and Social Change [i].

94 Tristan G Brown, Alexander Statman and Celine Sui, 'Public Debate on Facial Recognition Technologies in China' [2021] MIT Case Studies in Social and Ethical Responsibilities of Computing <https://mit-serc.pubpub.org/pub/public-debate-on-facial-recognition-technologies-in-china/release/1> accessed 1 August 2025.

95 Eva Erman and Markus Furendal, 'Artificial Intelligence and the Political Legitimacy of Global Governance' (2024) 72 Political Studies 421."plainCitation":"Eva Erman and Markus Furendal, 'Artificial Intelligence and the Political Legitimacy of Global Governance' (2024

96 Lilian Edwards, 'Regulating AI in Europe: Four Problems and Four Solutions (Ada Lovelace Institute Expert Opinion)' (*Social Science Research Network*, 1 March 2022) <https://papers.ssrn.com/abstract=5026691> accessed 2 September 2025; Nathalie A Smuha and others, 'How the EU Can Achieve Legally Trustworthy AI: A Response to the European Commission's Proposal for an Artificial Intelligence Act' (*Social Science Research Network*, 5 August 2021) <https://papers.ssrn.com/abstract=3899991> accessed 2 September 2025; Alice Giannini and Sarah Tas, 'AI Act and the Prohibition of Real-Time Biometric Identification' [2024] Verfassungsblog <https://verfassungsblog.de/ai-act-and-the-prohibition-of-real-time-biometric-identification/> accessed 2 September 2025.1 March 2022

97 Schneeberger and others (n 88).

98 ibid.

99 See also Recitals 20 and 27.

100 Bordt and others (n 89); S Wachter, B Mittelstadt and L Floridi, 'Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation' (2017) 7 International Data Privacy Law 76.B Mittelstadt and L Floridi, \\uc0\\u8216{}Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation\\uc0\\u8217{} (2017

principles but frames it alongside state priorities like social stability and 'controllability'.[101] This approach hints at a more state-supervised notion of transparency. The U.S. (through NIST and IEEE initiatives) often treats explainability as a technical feature to manage risk and improve trust, although without legally mandating explanations in the way the EU does.[102] Indeed, US-led efforts focus on voluntary risk management standards rather than hard requirements.[103] Such differences emerged at an SC 42 workshop where experts from ISO and CEN/CENELEC compared definitions and highlighted varying accents on interpretability versus user comprehension in explainability policies across the EU, US, and others.[104]

3. Risk Management

49 AI risk management presents another ground for normative divergence. The US's NIST AI Risk Management Framework (AI RMF) includes guiding principles like transparency, accountability and fairness, but it does not include fixed metrics for measuring them.[105] For its part, much of the existing ISO/IEC work on AI risk management has focused on organisational processes and governance structures, rather than product-oriented risks to individuals. This approach is described as having a broad and unspecific focus on organizational risks, and limited presence of risks to fundamental rights.[106] On the other hand, the EU Regulation makes a lifecycle-based risk management system the core compliance obligation for high-risk AI (Article 9) and, thus, goes beyond traditional product safety to encompass fundamental rights impacts as well as technical safety. The upcoming harmonised standards under the AI Act can be seen as more formalised compliance mechanisms.[107] Draft work items discussed in early 2024 suggest efforts to standardise not only risk classification but also obligations for post-market monitoring and incident logging.[108] More specifically, the forthcoming standards will concretely specify how high-risk AI providers must implement quality management systems, maintain audit logs, monitor incidents and update safety mechanisms over time. In short, they will translate general requirements into enforceable technical norms. Unlike other voluntary and principle-based NIST RFM, European harmonised standards are built to deliver presumption of conformity and, thus, impose specific mandatory compliance workflows and traceability specifications.[109]

50 China's approach on risk management also diverges from the EU approach. Its 2023 AI Security Assessment Guidelines, issued by the Cyberspace Administration of China (CAC), mandate pre-deployment security assessments for AI services that affect 'public-opinion attributes or social mobilization capabilities', which are criteria defined broadly enough to trigger mandatory ideological review and compliance clearance before public launch.[110] These assessments require organisations to submit formal reports to CAC and public security authorities, which evaluate potential risks to national security and social stability to assess that the concerned AI system is in line with core socialist values.[111] As such, the Chinese approach effectively turns risk governance into a tool of state oversight rather than a compliance mechanism. The divergence is thus institutional as well as substantive. While the EU seeks to operationalise explainability

101 Jeffrey Ding, Paul Triolo and Samm Sacks, 'Chinese Interests Take a Big Seat at the AI Governance Table' (*New America*, 20 June 2018) <http://newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/> accessed 1 August 2025.

102 Schneeberger and others (n 88).complex black box models such as GPT-4 have gained widespread adoption. Concurrently, explainable AI (XAI

103 Jose-Miguel Bello y Villarino and others, 'Standardisation, Trust and Democratic Principles: The Global Race to Regulate Artificial Intelligence' (*United States Studies Centre*, 31 July 2023) <https://www.ussc.edu.au/standardisation-trust-and-democratic-principles-the-global-race-to-regulate-artificial-intelligence> accessed 1 August 2025.

104 Ibid. See also Jeffrey Ding et al (n 95).

105 National Institute of Standards and Technology, 'Artificial Intelligence Risk Management Framework (AI RMF 1.0)' (NIST AI 100-1, 2023) DOI: 10.6028/NIST.AI.100-1.

106 Garrido Josep Soler and others, 'Harmonised Standards for the European AI Act' (*JRC Publications Repository*, 24 October 2024) <https://publications.jrc.ec.europa.eu/repository/handle/JRC139430> accessed 6 August 2025.

107 Commission Implementing Decision on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation in support of Union policy on artificial intelligence. Brussels, 22.5.2023. C(2023) 3215 final.

108 Garrido Josep Soler and others, 'Harmonised Standards for the European AI Act' (JRC Publications Repository, 2024 Garrido (n 107).

109 Ana Paula Gonzalez Torres and Timo Ali-Vehmas, 'AI Regulation: Maintaining Interoperability through Value-Sensitive Standardisation' (2025) 27 Ethics and Information Technology 26.

110 Esther Franks, Bianca Lee and Hui Xu, 'Report: China's New AI Regulations' (2024) 5 Global Privacy Law Review <https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\GPLR\GPLR2024007.pdf> accessed 4 August 2025.

111 Hui Xu and others, 'China's New AI Regulations' (*Latham & Watkins*, 16 August 2023) https://www.lw.com/admin/upload/SiteAttachments/Chinas-New-AI-Regulations.pdf accessed 30 March 2026.

and accountability through post-market monitoring standards, China enforces state-supervised oversight via mandatory pre-market assessment tied to political and social conformity.

4. Bias and Fairness

51 Bias mitigation has proven one of the most difficult areas to codify in standardisation, with frequent clashes over metrics and terminology. ISO/IEC TR 24027:2021 attempts to address bias in AI systems but avoids mandating specific thresholds, opting instead for a set of mitigation techniques.[112]

52 Within the AI Act context, fairness and bias are not left to voluntary guidance but embedded its provisions. Article 10 requires that training, validation and testing datasets be relevant, representative, free of errors and complete, thereby making data governance a legal tool for bias mitigation. Article 15 requires that high-risk AI systems be sufficiently accurate, robust and resilient against errors, which ties performance metrics directly to fairness outcomes. CEN-CENELEC JTC 21 has discussed audit and conformity-assessment frameworks that can operationalise these provisions for example, specifying documentation requirements for dataset representativeness, standardised metrics for accuracy across subgroups and procedures for logging and testing bias mitigation measures during system lifecycle.[113]

53 Chinese AI standards generally approach bias as a problem of model accuracy and rarely framing it in terms of rights or social justice.[114] In international standardisation, Western delegations have repeatedly called for inclusion of different impact assessments and protected category monitoring, which are terms that have met resistance on the grounds of cultural incompatibility and regulatory overreach.[115] Empirical findings confirm that such normative gaps remain unbridgeable in practice because attempts to define concepts like fairness or explainability within SDOs have often stalled due to diverging assumptions about the purpose and limits of algorithmic governance.[116] These frictions reveal a wider epistemic incompatibility. Thus, whereas the EU legislator frames fairness as a rights-enforcing obligation, others treat it as a reputational or procedural ideal/aspiration.

E. Consensus Is Not Convergence

I. Impact on the Implementation of the AI Act

54 These examples illustrate real tensions that could affect the **alignment of AI-related standards and, hence, the global implementation of the EU rules.** The AI Act heavily relies on technical standards to elaborate on its high-level requirements (for transparency, risk management, accuracy, etc.). However, if those standards are the product of geopolitical compromise, they might not fully match the vision of the EU lawmaker. For instance, an *accuracy* standard that omits human rights or a *risk management* standard with loose transparency provisions could **reduce the EU's power in AI governance** by yielding ground to private and foreign interests. Indeed, whoever **"sets the rules of the game"** in standards may tilt the playing field. This is important because, as mentioned above, standards embed normative choices and those choices implicitly shape regulation. Aware of that, the European Commission, emphasised the need for European leadership in key SDO committees to promote EU values in the 2022 Standardisation Strategy.[117]

55 Several **key implications** emerge from these frictions. First, the **definitions in ISO foundational standards** (like the ISO 22989 definitions of bias, transparency, etc.) might be recycled in the EU context.[118] However, if these definitions are too vague, they could create legal uncertainty. For example, the EU AI Act's understanding of (the undefined in the AI Act) *explainability* could be undermined if an ISO standard adopted as harmonised standard defines *explainability* in an overly technical or narrow way. Divergent national positions in the standards negotiations (e.g. EU pushing for plain-language explanations vs. others opting for algorithmic

112 https://www.iso.org/standard/77607.html

113 James Davenport, 'CEN–CENELEC JTC21 and the EU AI Act Article 10 (Data)' (Lecture at the University of Bath, 27 June 2025) <https://people.bath.ac.uk/masjhd/Slides/BDVA202050627.pdf>.

114 Matt Sheehan, 'China's AI Regulations and How They Get Made'. (*Carnegie Endowment for International Peace*, 10July 2023)<https://carnegieendowment.org/research/2023/07/chinas-ai-regulations-and-how-they-get-made?lang=en> accessed 5 August 2025.

115 Sandra Wachter, Brent Mittelstadt and Chris Russell, 'Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI' (2021) 41 Computer Law & Security Review 105567.

116 Roberts and Ziosi (n 85).

117 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market*. Brussels, 2.2.2022 COM(2022) 31 final, at p. 4-6.

118 Article 40(3) AI Act.

transparency only) determine if an AI provider can tick a compliance box or must fundamentally change a system. Second, the **power dynamics in standard-setting** (largely dominated by Big Tech companies) increase the risk that standards favour industry convenience over strict accountability. If, for instance, US and Chinese tech companies manage to frame *accountability* in international standardisation as simply having an internal process and this becomes a harmonised standard, it may fall short of the AI Act's idea of transparency and human oversight. And lastly, there is the risk of standards conflicts becoming irreconcilable, in which the EU might reject certain international standards. While the EU generally prefers global standards, it will insist on modifications if values clash. This may result in 'EN-ISO' standards with EU-specific annexes, or even entirely European standards, although such lack of harmonisation would complicate compliance for companies operating globally.

56 Frictions can surface in meeting minutes and comment resolutions, but they are critical to monitor. However, in the effort to reach consensus, they will determine whether international AI standards become a model for global convergence or, instead, a loophole that allows regional values (like those enshrined in EU law) to be side-stepped. Here, the tension between EU and international standardisation becomes apparent. International SDOs are not bound by EU constitutional principles. They are consensus-based forums where geopolitical interests compete. Thus, when the EU adopts standards negotiated in those fora, it imports not only the technical content but also the institutional politics that shaped it. The risk is that the formal alignment (via harmonisation) may conceal substantive divergence, particularly where definitions, obligations or processes fall below EU expectations.

57 Accordingly, achieving consensus requires diluting normative ambition. This is especially salient in standardisation, where powerful actors, often industry coalitions or dominant states, can steer the process toward minimal, generic provisions.[119] Therefore, as seen, the need to maintain consensus often results in language that is procedurally precise but substantively hollow. For the EU, this means that harmonised standards may not meaningfully advance the AI Act's regulatory goals. For instance, if explainability is operationalised in purely technical terms to appease actors who reject legal redress or user-facing transparency, the standard may allow providers to meet compliance requirements without delivering meaningful protections.[120] The result is a regulatory structure vulnerable to capture and symbolic implementation.

58 In view of the above, in cases where international standards fall short, Europe is strengthening them or writing its own, e.g. with common specifications. Therefore, this is a clear instance where consensus does not equal cooperation. The EU cannot simply cooperate by adopting the ISO standard indiscriminately because the consensus result does not achieve the EU's policy goals. True cooperation would require other global players to also value and implement stricter measures, which is not yet the case.[121]

59 There are also instances where nominal consensus collapses under stress. Within ESOs processes, consensus is sought among member states, but conflicting views often surface during drafting and inquiry.[122] National committees can send opposing comments (for example, one country pushing for a stricter requirement, another for a looser one), which can result in compromises that satisfy neither. Thus, even when a harmonised standard is adopted, some participants might only reluctantly agree, and cooperation in actual rollout (e.g. promoting use of the standard nationally) may be lukewarm. This dynamic is amplified on the international stage: countries might agree to broad AI principles in an OECD or G20 context yet disagree on their implementation in domestic standards and laws. The failure of consensus to ensure convergence is evident in the divergent deployment of supposedly "agreed" norms. For instance, both the EU and China endorse fairness and transparency in AI at a high level[123] but, as seen above, they operationalise those concepts very differently.

60 Finally, the resulting divergence affects enforcement. If EU harmonised standards diverge significantly from Chinese or ISO standards, companies operating

119 Cf Kal Raustiala and Anne-Marie Slaughter, 'International Law, International Relations and Compliance' (Social Science Research Network, 1 November 2002) <https://papers.ssrn.com/abstract=347260> accessed 7 August 2025; Daniel W Drezner, *All Politics Is Global : Explaining International Regulatory Regimes* (Princeton University Press 2008) <https://www.torrossa.com/en/resources/an/5641442> accessed 7 August 2025.

120 Brady Lund and others, 'Standards, Frameworks, and Legislation for Artificial Intelligence (AI) Transparency' (2025) 5 AI and Ethics 3639; Högberg (n 4).

121 Bello y Villarino and others (n 103).

122 'Standard-setting Overview' (*Artificial Intelligence Act*, 16 December 2022) <https://artificialintelligenceact.eu/standard-setting-overview/> accessed 30 March 2026.

123 Ministry of Foreign Affairs of the People's Republic of China, 'Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (AI)' (17 November 2022) <https://www.fmprc.gov.cn/eng/zy/wjzc/202405/t20240531_11367525.html> accesed Mrch 25th 2026.

across jurisdictions may struggle to comply with all the existing standards at once, which potentially results in a standards battle. This could undermine the cooperative spirit in the AI Act (Article 40(3)), which stresses international cooperation on standardisation. Yet, in practice, the EU might reject an international standard for not meeting its normative benchmark. The challenge is to strive for consensus that reflects shared high ambitions, rather than the lowest common denominator.[124] Therefore, where consensus fails, the resulting patchwork reveals the fault lines of global AI governance.

II. The Future of the EU AI-related Standardisation

61 The EU approach to AI standardisation is bound to the structural and geopolitical realities of global standardisation. As this paper has shown, the AI Act's reliance on, eventually 'harmonised', standards, many of which are beng developed in international forums, makes the effectiveness of the AI Act partly dependent on **institutions the EU does not control.** The result is a structural normative incompatibility. On the one hand, it promotes AI regulation grounded in fundamental rights and accountability. On the other hand, the technical norms that will operationalise this vision are often shaped in fora dominated by corporate interests and negotiated through geopolitical compromise. This gap between **regulatory ambition and infrastructural dependency** raises urgent questions about the future direction of EU AI standardisation. Different scenarios are possible.

62 In the best-case scenario, the EU succeeds in shaping international standards in a way that reflects its legal values. This would require sustained leadership within international SDOs, effective mandates to ESOs and a more meaningful representation of public interest actors. If global standards evolve, in line with the EU vision, to embed stronger rights protection and accountability mechanisms, international harmonisation could both support the AI Act and advance global convergence. This scenario, however, is quite unlikely given the current geopolitical scenario.

63 More realistically, the EU may need to **selectively decouple** from international standards that fall short of its regulatory (and normative) goals. This could involve developing EU-specific annexes, issuing supplementary guidance or using common specifications under Article 41 to fill normative gaps. Such a strategy could preserve internal coherence but would complicate cross-border compliance and might reduce the EU's influence in global AI governance.

64 A more concerning scenario is that normative and strategic differences deepen and eventually result in incompatible regulatory regimes. If international standards remain too generic or are co-opted by commercial interests in a way that the EU is forced to reject them entirely, global firms may face multiple, conflicting standards. In addition to increase compliance costs and create market fragmentation, this scenario could weaken the EU's ability to influence global norms and diminish interoperability in critical AI infrastructures. Over time, such fragmentation could also further erode trust in the legitimacy of technical governance and undermine the very values that the EU seeks to embed in AI regulation.

65 Moreover, while the AI Act relies on harmonised standards to refine its broad requirements, the standardisation process has proven s**lower** than anticipated. The European Commission's, first then repealed, formal standardisation request issued in 2023, initially set a tight deadline that targeted the completion of dozens of new standards by April 2025. Yet that timeline has slipped considerably. As of early 2026, the work had fallen behind. The **ESOs** have conceded that many AI standards will only be finalized by late 2026 and media reports indicate that **most will not be ready until after** the AI Act's own compliance dates in August 2026.[125] This delay is problematic, as it leaves companies little time to adapt before the full entry into force of the Regulation. As a result, as part of the broader Digital Omnibus on AI proposal, the Commission has indicated that the application of high-risk AI obligations should be tied to the availability of these support instruments, with full compliance potentially postponed beyond the original August 2026 deadlines and into 2027 or later.[126]

66 In the meantime, Europe cannot simply rubber-stamp existing ISO/IEC standards as a solution. It must adapt or rewrite them to align with EU values and legal mandates. While international AI standards provide a starting point, EU experts have found that they only partially cover the Act's stringent requirements for 'trustworthy AI' especially those tied to

124 Andrew L Russell, 'Open Systems and the Limits of Democratic Design, 1970s–1980s', in *Open Standards and the Digital Age: History, Ideology, and Networks* (Cambridge University Press 2014).

125 https://artificialintelligenceact.eu/standard-setting. The revised Standardisation Request (C(2025) 3871 final) acknowledges significant delays in the execution of the initial mandate and responds by imposing a compressed and closely monitored timeline for the completion of harmonised standards.

126 COM(2025) 836 final.

fundamental rights.[127] The European Commission's Joint Research Centre, in reviewing the standards gap, has highlighted numerous areas where global standards fall short and new or augmented European standards are needed.[128] Transparency, logging, and data governance are notable examples: ISO's AI management system standard (ISO/IEC 42001) treats logging and record-keeping as optional risk controls, whereas the AI Act makes robust record-keeping a legal obligation.[129] To bridge such gaps, CEN-CENELEC's JTC 21 is drafting standards that will mandate traceability, transparency documentation, data quality metrics and other features specifically demanded by EU law.[130] This need to "patch" or supplement international standards is useful to map where global consensus is too insufficient to meet Europe's higher bar.

67 Read together, the future scenarios outlined above call into question the assumption that global convergence through standardisation is either inevitable or normatively desirable. Where consensus-based standard-setting processes dilute substantive regulatory commitments, fragmentation may represent not regulatory failure but a governance outcome reflecting persistent normative disagreement. From this perspective, the EU's reliance on standardisation can be seen less as a project of exporting uniform rules and more as an effort to sustain normatively meaningful regulation in a plural and contested global environment. Accordingly, the gap between extraterritorial regulatory ambition and infrastructural dependency also tempers expectations associated with the EU's ability to effectively externalise its regulatory preferences through market size alone. Where the operational content of legal obligations is mediated through transnational standardisation processes, regulatory influence cannot be assumed to flow unidirectionally from legal ambition or market power.

68 Ultimately, the future of EU AI standardisation will depend not on the AI Act's text itself, but on who defines its operational meaning in the standardisation arena. In contexts where procedural consensus erodes thresholds, narrows definitions and sidelines independent oversight, "compliance" risks becoming a checklist detached from the Act's normative core. These are, unfortunately, structural features of consensus-based global governance.[131] If the EU treats SDOs as neutral technical spaces, it risks yielding control over the law's substance to actors with different priorities. If it instead consistently treats them as fora of (geo)political contestation, standardisation can serve to project EU legal commitments in global AI governance.[132]

F. Conclusions

69 The emerging transnational legal order for AI cannot be evaluated against the familiar backdrop of national legal systems' formalism or their constitutionalising trajectories without recognising the simultaneous fragmentation of international law and the resulting global legal pluralism. This pluralism is not an abstract feature of the global AI governance, instead it is visible in the technical details and institutional arrangements through which AI is actually being regulated. The question is therefore not simply whether AI should be governed through national or transnational law, but what kind of legal order can sustain effective regulation in an environment where competing governance models seek to project their norms globally.

70 China's latest move to create a 41-member AI standardisation technical committee, featuring executives from Baidu, Alibaba Cloud, Tencent, Huawei, SenseTime, Ant Group and top universities is an explicit turn towards enterprise-led, yet state-coordinated, governance of AI infrastructure.[133] The committee is tasked with drafting standards for large language models, datasets, AI risk assessment and software platforms, with an aim to prepare at least 50 new standards by 2026.[134] For its part, the AI Act is a test case for the EU's capacity to legislate in a manner that is both transnational in reach and resilient against the commercial, technological and (geo)political pressures that shape AI governance.

71 However, as things currently stand, the EU approach to standardisation appears inherently fragile. The (internal and external) legitimacy and effective reach of the AI Act will depend on standards authored by SDOs that the Union does not control.

127 Gornet (Mélanie) and Maxwell (Winston), 'The European Approach to Regulating AI through Technical Standards' (2024) 13 Internet Policy Review <https://policyreview.info/articles/analysis/regulating-ai-through-technical-standards> accessed 7 August 2025.

128 Soler and others (n 106).

129 Ibid.

130 Ibid.

131 Drezner (n 119).

132 Cf Fabrizio Cafaggi and Katharina Pistor, 'Regulatory Capabilities: A Normative Framework for Assessing the Distributional Effects of Regulation' (2015) 9 Regulation & Governance 95.

133 Zeyi Yang and Knight, Will, 'Inside the Summit Where China Pitched Its AI Agenda to the World' (*Wired*, 31 July 2025) <https://www.wired.com/story/china-artificial-intelligence-policy-laws-race/> accessed 8 August 2025.

134 Junhua Zhu, 'China's Approach to AI Standardisation: State-Guided but Enterprise-Led' (2024) Finnish Institute of International Affairs. *FIIA Briefing Paper* n 391 (08/2024).

As the research suggests, within those, procedural consensus frequently conceals deep normative and strategic fractures, with core safeguards on explainability, fairness and bias auditing running the risk of being diluted (or erased altogether) to secure agreement. In a context in which the relevance of standardisation as a tool for governance is growing, involvement in standard-setting still shapes outcomes, but the asymmetric participation is stark. Civil society and SMEs remain marginal, while corporate or other normatively incompatible interests dominate the deliberations. In addition to this unresolved asymmetry, we need to consider the structural pacing problem. The 2026 target for the delivery of harmonised standards is set against looming AI Act compliance deadlines. This tight timeline risks leaving the EU's normative ambitions hostage to incomplete or externally steered technical regimes.

72 The research suggests that the politics of depoliticisation and re-politicisation in the AI Act's delegation to standardisation are driven both by internal market integration logics and by the need to uphold regulatory hegemony. The inclusion of common specifications in the AI Act offers a potential institutional counterweight. In the EU legal order, common specifications operate as a safety net in areas such as medical devices and cybersecurity, allowing the European Commission to adopt directly applicable technical requirements that ensure presumed conformity without relying on external SDOs. Their deployment in AI governance would enable the Union to safeguard its legislative intent when global consensus dilutes substantive protections or delays their delivery. This mechanism, however, has been underexplored in both policy and scholarship, and its role in preserving normative control in a fragmented international standardisation landscape warrants closer legal analysis.

73 From an institutional perspective, the analysis points to a set of design tensions that any future configuration of EU AI standardisation will need to address. These include, first, the appropriate scope of standardisation. In particular, whether harmonised standards should continue to operationalise normatively dense obligations, or whether such requirements should be retained at a more centralised level of legal specification. Second, they concern the allocation of regulatory functions between decentralised standard-setting bodies and public authorities, including the conditions under which instruments such as common specifications should be deployed as ordinary tools of governance rather than exceptional fallbacks. Third, they raise questions about the functional differentiation of standards, especially where technical interoperability and measurement are intertwined with infrastructural control over data, models or system architectures. Finally, the findings suggest a need for further legal analysis of how reliance on transnational standardisation affects regulatory adaptability over time, and of the institutional consequences of partial or selective decoupling from international standards where consensus fails to sustain substantive legal commitments.