jipitec

1| 2026

Volume 17(2026)
Issue 1 ISSN 2190-3387

Special Issue on Harmonised Standards in AI Regulation

Journal of Intellectual Property, Information Technology, and Electronic Commerce Law

www.jipitec.eu

2026

jipitec

Journal of Intellectual Property, Information Technology and Electronic Commerce Law

Volume 17 Issue 1 May 2026
www.jipitec.eu
contact@jipitec.eu

A joint publication of:

Prof. Dr. Thomas Dreier, M. C. J. (NYU)
KIT - Karlsruher Institut für Technologie, Zentrum für Angewandte Rechtswissenschaft (ZAR), Vincenz-Prießnitz-Str. 3, 76131 Karlsruhe Germany

Prof. Dr. Axel Metzger, LL. M. (Harvard)
Humboldt-Universität zu Berlin, Unter den Linden 6, 10099 Berlin

Prof. Dr. Gerald Spindler (†)
Dipl.-Ökonom, Georg-August-Universität Göttingen, Platz der Göttinger Sieben 6, 37073 Göttingen

Karlsruhe Institute of Technology, Humboldt-Universität zu Berlin and Georg-August-Universität Göttingen are corporations under public law, and represented by their respective presidents.

ISSN 2190-3387

Funded by
DGRI Deutsche Gesellschaft für Recht und Informatik e.V.

Table Of Contents

Editorial

Articles

Editorial

by **Annalisa Volpato, Mariolina Eliantonio and Michèle Finck ***

Recommended citation: Annalisa Volpato, Mariolina Eliantonio and Michèle Finck, Editorial, 16 (2026) JIPITEC 1 para 1.

Harmonised Standards in AI Regulation: An Introduction to the Special Issue

I. Introduction

1 The adoption of the Regulation on Artificial Intelligence ("AI Act") represents a major milestone in the European digital strategy. With its entry into force in August 2024, the EU is one of the first legal systems[1] to have adopted a comprehensive framework for regulating the development, the placing on the EU market, and the use of artificial intelligence ("AI") systems, while addressing the impact of AI on the fundamental rights of individuals, such as human dignity, the right to privacy, the protection of personal data and freedom of expression, and on societal values, including democracy, the rule of law, and the protection of the environment.

2 The actual implementation of this legislative framework, however, will require extensive technological expertise to further detail specific rules for producers and users of AI. For this reason, the EU institutions will heavily rely on the regulatory work of international and European standardisation organisations which have already been developing technical standards on artificial intelligence.[2] As stated by the European Commission, standardisation organisations are meant to lead the path for the digital transition of the EU economy by elaborating detailed specifications in support of EU legislation.[3] In particular, the AI Act expressly refers to harmonised standards for the operationalisation of the requirements for high-risk systems and, to a certain extent, for general-purpose AI models, establishing a presumption of conformity for systems and models compliant with them.[4]

3 While this regulatory technique makes the role of technical standards as complementary tools vis-à-vis EU regulation clearly visible,[5] it also shows that they do not only regulate technical and scientific aspects of AI and its value chains, but also have

* Annalisa Volpato, Associate Professor of European Union law, University of Padova; Mariolina Eliantonio, Professor of European and Comparative Administrative Law and Procedure, Maastricht University; Michèle Finck, Professor of Law and Artificial Intelligence and Director, CZS Institute for Artificial Intelligence and Law, University of Tübingen.

1 Compare the scope of the AI Act with the US AI Bill of Rights (2022); Executive Order on the Safe, Secure, and Trustworthy Development and Use of AI (2023); and with Chinese Law on Generative AI (2023).

2 See, inter alia, Andrew Leyden, 'Standards and the EU AI Act: Legitimacy, state of play, and future challenges' (2025) *Information & Communications Technology Law* 1.

3 See European Commission, *Communication: Shaping Europe's digital future*, Publications Office of the European Union, 2020, 7. See also Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, OJ 2022 L 323/4.

4 Art. 40 and 55 AI Act.

5 Irene Kamara, *Standardizing Personal Data Protection* (Oxford University Press 2025)

the potential to influence and express broader value policy choices.[6] As Majone has aptly put it, standards are "a microcosm in which conflicting epistemologies, regulatory philosophies, national traditions, social values, and professional attitudes are faithfully reflected".[7] At the same time, standard-setting at the international level is acquiring a stronger geopolitical meaning.[8] With some third states taking an unprecedentedly assertive stance to standardisation, the latter becomes a contentious terrain where the EU struggles to safeguard its values and interests in standard-setting against an increasingly competitive global context.[9]

4 Although the role of harmonised standards in the AI Act is gaining increasing attention in academic debate,[10] the interplay between the current dynamics in technical standardisation and the democratic guarantees that the implementation of the AI Act needs to abide by, has arguably not been sufficiently explored in the literature. The involvement of technical standardisation in the regulation of the AI Act raises a number of legal and non-legal questions pertaining to their role, their effects, and the control that public institutions and civil society can exercise on their activities. The unprecedented geopolitical, fundamental rights and ethical considerations enshrined in AI standardisation give new dimensions to these questions and thus deserve further scholarly attention. This is precisely the purpose of this special issue.

5 This introduction will provide an overview of the historical development of the New Approach and how, from a product regulation logic, standardisation found its way into digital regulation generally and the AI Act specifically. Moreover, it will outline the primary questions addressed and posit the central hypothesis of this special issue: that, as it acquires an unprecedented legal, ethical and geopolitical dimension, the use of technical standardisation in the field of AI represents a shift in the role of harmonised standards in EU law and this poses novel challenges to their legitimacy within the EU socio-legal order.

II. Harmonised Standards and EU Law: From Industrial Products to AI Regulation

6 The use of technical standardisation for the purpose of complementing and operationalising EU regulation is not a new regulatory technique in EU law. Since 1985, the EU legislator has relied on these – formally – non-binding, voluntary instruments in the regulation of the European market for industrial products through the so-called "New Approach". The New Approach (now refined in the New Legislative Framework) consists of regulating through legislative acts only the essential requirements of general interest of a product, while referring the detailed definition of technical aspects to private standardisation organisations.[11] The different steps are now set forth in the so-called Standardisation Regulation.[12] Accordingly, after the adoption of a legislative act, the European Commission issues a request to one or more European standardisation organisations to elaborate a document defining the technical requirements to be fulfilled by a product,

6 See Giandomenico Majone, 'Science and Trans-Science in Standard Setting' (1984) 9 *Science, Technology, & Human Values* 15; Sheila Jasanoff, 'Epistemic Subsidiarity – Coexistence, Cosmopolitanism, Constitutionalism' (2013) 4(2) *European Journal of Risk Regulation* 133.

7 Giandomenico Majone, *ibid*, 15.

8 See further Mélanie Gornet and Hélène Herman, 'A peek into European standards making for AI: between geopolitical and economic interests' (2024), hal-04784035. See also Cantero in this special issue.

9 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, 1 and 5. See also Marta Cantero Gamito, 'The influence of China in AI governance through standardisation' (2023) 47(10) *Telecommunications Policy*, 102673.

10 See, in particular, Sybe de Vries, Olia Kanevskaia and Rik de Jager, 'Internal Market 3.0: The Old 'New Approach' for Harmonising AI Regulation' (2023) 8(2) *European Papers*, 583; Andrew Leyden, above n 2, 1; Marta Cantero Gamito and Christopher Marsden, 'Artificial intelligence co-regulation? The role of standards in the EU AI Act' (2024) 32 *International Journal of Law and Information Technology*, eaae011; Marco Almada and Nicolas Petit, 'The EU AI Act: A medley of product safety and fundamental rights?' (2023) 59 EUI Working Papers.

11 See Commission of the European Communities, *Completing the Internal Market. White Paper from the Commission to the European Council,* Milan, 28-29 June 1985, COM(85)310 final; Council Resolution of 7 May 1985 on a new approach to technical harmonization and standards, OJ 1985, C 136/1; Council Resolution of 21 December 1989 on a global approach to conformity assessment, OJ 1990, C 10/1; Regulation (EU) No 1025/2012 on European Standardisation, OJ 2012, L 316/12.

12 Regulation 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, OJ 2012, L 316/12. See also Regulation (EU) 2022/2480 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 1025/2012 as regards decisions of European standardization organisations concerning European standards and European standardization deliverables, OJ 2022, L 323/1.

process, service or system. The standards are then elaborated by the European standardisation organisations and sent to the European Commission. These standards, adopted on the basis of a request made by the Commission for the application of Union harmonisation legislation, are defined as "harmonised standards". If the Commission concludes that the standard is in compliance with the request and Union legislation, it publishs its reference in the Official Journal of the European Union. This publication provides a presumption of conformity with the legislative standards they are linked to.

7 The use of technical standards in EU legislation has rightfully attracted scholarly attention, initially from economists[13] and political scientists,[14] and more recently from legal scholars.[15] Technical standards elaborated by private European standardisation bodies are in theory voluntary and non-binding, in the sense that an economic operator can always prove the conformity of their products with EU legislation by providing evidence of their compliance with the essential requirements of safety in a different way. However, the presumption of conformity attached to the compliance with a harmonised standard has in practice relevant legal effects beyond the private sphere. Previous research has shown that, considering the legislative and regulatory context in which the standard-setting bodies operate, and the actual practice of the market, it is very difficult and expensive for the economic operators to prove the conformity of their products to the essential requirements of harmonisation legislation in a different way.[16] As confirmed by the Court of Justice of the European Union (CJEU), in certain cases voluntary standards issued in connection with legislation can be considered *de facto* binding.[17] Recent political[18], legal[19] and jurisprudential[20] developments in the EU have put the debate on the tight integration between the law and private technical standards in the spotlight.

8 In the light of this progressive "juridification" of harmonised standards,[21] seminal EU public law literature has questioned the legality of the delegation of regulatory powers to private bodies in the light of the strict limits established by the case law of the CJEU.[22] Others have focused on the more specific violations of EU rules on fair competition and intellectual property which technical standardisation may cause.[23] Finally, stark criticism

13 See inter alia, Franklin Edward Powell, *Some Aspects of Standardization and Economic Theory* (Catholic University of America 1947); H Landis Gabel, *Product Standardization and Competitive Strategy* (Elsevier Science 1987); H Landis Gabel, *Competitive Strategies for Product Standards: The Strategic Use of Compatibility Standards for Competitive Advantage* (McGraw-Hill 1991); Peter Grindley, *Standards, Strategy, and Policy: Cases and Stories* (Oxford University Press 1995); Carmen Matutes and Pierre Regibeau, 'A Selective Review of the Economics of Standardization. Entry Deterrence, Technological Progress and International Competition' (1996) 12(2) *European Journal of Political Economy* 183. More recently, see Knut Blind, *The Economics of Standards: Theory, Evidence, Policy* (Edward Elgar 2004).

14 Susanne K Schmidt and Raymund Werle, *Coordinating Technology: Studies in the International Standardization of Telecommunications* (MIT Press 1998); Kenneth W Abbott and Duncan Snidal, 'International Standards and International Governance' (2001) 8(3) *Journal of European Public Policy* 345; Tim Büthe and Walter Mattli, 'Setting International Standards: Technological Rationality or Primacy of Power?' (2003) 56(1) *World Politics* 1; Tim Büthe and Walter Mattli, 'International Standards and Standard-Setting Bodies' in David Coen, Wyn Grant, and Graham Wilson (eds), *The Oxford Handbook of Business and Government* (Oxford University Press 2010) 440; Tim Büthe and Walter Mattli, *The New Global Rulers: The Privatization of Regulation in the World Economy* (Princeton University Press 2011).

15 Harm Schepel, *The Constitution of Private Governance. Product Standards in the Regulation of Integrating Markets* (Hart 2005); Günther Teubner, *Constitutional Fragments: Societal Constitutionalism under Globalisation* (Cambridge University Press 2012).

16 See, inter alia, Mariolina Eliantonio and Caroline Cauffman (eds), *The Legitimacy of Standardization as a Regulatory Technique A Cross-disciplinary and Multi-level Analysis* (Edward Elgar 2020); H Schepel, above n 15; Jacques Pelkmans, 'The New Approach to Technical Harmonisation and Standardization' (1987) 25(3) *Journal of Common Market Studies* 249.

17 See Case T-474/15, *Global Garden*, EU:T:2017:36, para 67; Case C-171/11, *Fra.bo. v DVGW*, EU:C:2012:453. See also Case C-367/10 P, *EMC*, EU:C:2011:203.

18 European Commission, *An EU Strategy on Standardization*, above n 9.

19 Regulation (EU) 2022/2480 of the European Parliament and of the Council of 14 December 2022 amending Regulation (EU) No 1025/2012 as regards decisions of European standardization organisations concerning European standards and European standardization deliverables, OJ 2022, L 323/1.

20 *Inter alia*, Case C-588/21 P, *Public.Resource.Org*, EU:C:2024:201; Case C-160/20, *Stichting Rookpreventie Jeugd*, EU:C:2022:101.

21 Hans-W. Micklitz and Rob van Gestel, 'European integration through standardization: How judicial review is breaking down the club house of private standardisation bodies', (2013) 50(1) *Common Market Law Review* 145.

22 Christian Joerges, Harm Schepel and Ellen Vos, *The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardization under the New Approach* (European University Institute 1999).

23 Pierre Arhel, 'Comportements anticoncurrentiels dans le cadre de la normalisation' (2010) 147 *Petites affiches*, 4; François Lévêque, 'La normalisation et le droit de la concurrence face au hold-up' (2007) *Revue Lamy de la concurrence*, 170-175; Björn Lundqvist, 'European

was raised with regard to the lack of transparency and participation of the standard-setting process, as well as in relation to the lack of access to the text of standards for the public, and of procedural guarantees to counter-balance the regulatory capture by big companies.[24]

9 Despite the academic criticism towards the mechanism of referencing to harmonised standards in EU legislation, the supranational legislator has decided to follow this well-established regulatory technique of the New Approach - which has proven undoubtedly successful in the regulation of the internal market for industrial products – in the regulation of a vast, value-loaded and cutting-edge field such as that of digital technologies. References to harmonised standards are included in many recent legislative acts in the field, including the Data Act,[25] the Cyber Resilience Act,[26] and - most importantly for the purpose of this special issue - the AI Act. In fact, Articles 32, 42 and 53 of the AI Act establish a presumption of conformity for AI systems and general-purpose AI models which comply with harmonised standards. This entails that, in particularly sensitive sectors, such as education, critical infrastructures, justice and employment,[27] the precise rules to ensure compliance with the requirements set in the AI Act - concerning, for instance, risk management, the quality and relevance of data sets used, and human oversight[28] - will be *de facto* spelled out by European standardisation organisations. CEN and CENELEC have received the request to issue the relevant harmonised standards from the European Commission on 22nd May 2023[29] and are currently developing them in five working groups within the Joint Technical Committee 21 (JTC21).[30]

III. Harmonised Standards and the AI Act: A Paradigm Shift and New Challenges

10 The decision of the EU co-legislators to rely on harmonised standards in the AI Act not only transplants the same legal issues that the academic community had highlighted in relation to the regulation of industrial products according to the New Approach to the digital regulation field, but also represents a fundamental shift in the role of technical standards in EU law, as has been acknowledged by the EU institutions[31] and by the standardisation community itself.[32] The object of this form of private regulation will be inevitably imbued with value judgments and sensitive implications, in particular as standards will explicitly have to address fundamental rights.[33]

11 This special issue gives an interdisciplinary account of this highly topical development, bringing together scholars with legal, socio-political and philosophical backgrounds. Thus, while most contributions are based on a legal doctrinal approach[34] and draw from

Harmonised Standards as 'Part of EU Law': The Implications of the James Elliott Case for Copyright Protection and, Possibly, for EU Competition Law' (2017) 44(4) *Legal Issues of Economic Integration* 421.

24 Mariolina Eliantonio, 'Judicial Control of the EU Harmonized Standards: Entering a Black Hole?' (2017) 44(4) *Legal Issues of Economic Integration*, 399-404; Carlo Tovo, 'Judicial Review of Harmonised Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU Law' (2018) 55(4) *Common Market Law Review*, 1187-1216; Carlo Colombo and Mariolina Eliantonio, 'Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?' (2017) 24(2) *Maastricht Journal of European and Comparative Law*, 323-340; Mariolina Eliantonio and Megi Medzmariashvili, 'Hybridity Under Scrutiny: How European Standardization Shakes the Foundations of EU Constitutional and Internal Market Law' (2017) 44(4) *Special issue of the Legal Issues of Economic Integration*.

25 Art. 33 of Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), OJ L 2023, 2854.

26 Art. 27 of Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements, OJ L 2024, 2847.

27 The full list of sectors can be found in Annex III. See also Art. 6 AI Act.

28 As well as technical documentation and record-keeping, transparency and the provision of information to deployers, human oversight, and robustness, accuracy and cybersecurity, see Art. 8-27 AI Act.

29 Thus, before the adoption of the AI Act, see European 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, C(2023) 3215 final.

30 See https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/.

31 European Commission, above n 9.

32 Dermott Jewell, Speech at the first meeting of the High-Level Forum on European standardization, 20 January 2023.

33 See, inter alia, Marion Ho-Dac, 'The EU AI Act and the challenge of protecting fundamental rights' (2025) 62(5) *Common Market Law Review*, 1299 – 1336.

34 Jan M Smits, 'What Is Legal Doctrine? On the Aims and Methods of Legal-Dogmatic Research' in Rob van Gestel, Hans-Wolfgang Micklitz and Edward L Rubin (eds), *Rethinking Legal Scholarship: A Transatlantic Dialogue* (Cambridge University Press 2017), 210.

political, ethical, societal considerations[35] in order to place AI standardisation in its social, economic, political and cultural context,[36] others employ empirical or theoretical methodologies. From this interaction between different perspectives on the topic, the multifaceted and transversal meaning and value of the role of technical standardisation in AI regulation, as well as the risks arising from it, clearly emerge.

12 As highlighted in the contribution of **Elvira Maria Rosaria Oliva**, the role of harmonised standards is particularly crucial in complementing the architecture foreseen for the protection of fundamental rights in the AI Act. In particular, she notes that in the AI Act fundamental rights function not only as legal parameters for harmonised standards, but also as a criterion to categorise AI systems and, consequently, the applicable legal regime. However, the assessment of a possible violation of fundamental rights is necessarily context-specific, which sets the AI Act apart from "the static and quantitative logic"[37] of the traditional product regulation where harmonised standards have traditionally been employed. Furthermore, AI systems may affect a plurality of fundamental rights, requiring a complex balancing exercise. Oliva thus raises doubts as to whether entrusting ESOs with fundamental right compliance respects the limits of the *Meroni* delegation doctrine,[38] especially in light of the limited judicial control over harmonised standards by the CJEU.

13 The vague requirements of the AI Act are difficult to operationalise and thereby pose fundamental "decision problems" not only for ESOs but also for regulatees because they require implementation through value judgments and evidence assessment under conditions of uncertainty, as argued by **Alessio Tartaro, Arvin Obnasca** and **Enrico Panai**. They link this issue specifically to the contestability of several essential requirements of the AI Act and the epistemic dependence this entails. The potential misalignment between the logic of the New Legislative Framework which was conceived for product regulation - where such "decision problems" are of a different nature and of lesser complexity - and the realities of AI governance brings, in their view, the risk of undermining the regulatory effectiveness of the AI Act. They, therefore, propose procedural steps aimed to introduce a body of evidence and argumentation, as part of the relevant technical documentation, "that explicitly demonstrates how the regulatee has identified, analysed, deliberated upon, and resolved the key decision problems pertinent to their specific high-risk AI system in order to meet the Act's essential requirements" [39]

14 The increasing ethical dimension of technical standardisation is also discussed by **Simone Casiraghi** and **Niels van Dijk** who examine the 'ethification' of technical standards and the institutionalisation of ethics through international standardisation on AI, exploring the challenges raised by this development in particular in relation to the Institute of Electrical and Electronics Engineers (IEEE). This examination of the politics of ethical standards in the governance of AI focuses on two elements: first, how ethics change through standardisation and, second, the mutual roles for risk producers, assessors and bearers in the use of ethical standards for governing AI risks. They argue that ethics standards, while they promise to offer a more responsible way to govern AI, transform ethics into an engineering requirement modelled on the procedures, language and logic of operationalisation of standardisation, exacerbating the traditional challenges related to representation, accountability, enforcement and transparency.

15 Finally, as underlined also in the 2022 EU Standardization Strategy,[40] international standardisation of digital technologies - and AI in particular - is currently characterised by complex geopolitical tensions, with competing "digital empires"[41] and other standardisation organizations active in the field. The outcome of these geopolitical frictions in international organisations, such as the International Organisation for Standardisation (ISO) and the Institute of Electrical and Electronics Engineers (IEEE), traditionally more vulnerable to regulatory capture by multinational corporations, will almost inevitably influence - in different ways and to different extents - the implementation of the AI Act in the EU. This dimension is explored in particular in the contribution by **Marta Cantero**, highlighting the role of standards for governing critical infrastructure and the influence of external regulatory dynamics in shaping legal structures. Her analysis of the impact of global (geo-) political dynamics on AI standardisation showcases that reliance on standardisation offers the EU an opportunity for global influence and resilience against changing dynamics, but it also generates a situation of vulnerability as procedural consensus

35 Bruno De Witte, 'Legal Methods for the Study of EU Institutional Practice' (2022) 18(4) *European Constitutional Law Review*, 639-640.

36 Francis Snyder, 'Establishing Law in Context: An Insider's Perspective' (Verfassungsblog, 20 April 2024). See also Agustín J Menéndez, 'The Triumph of EU Law in Context?' (Verfassungsblog, 22 April 2024).

37 Oliva in this special issue.

38 Case C-10/56 *Meroni v High Authority of the European Coal and Steel Community [1958] EU:C:1958:7.*

39 Tartaro et al. in this special issue.

40 European Commission (n 9).

41 Anu Bradford, *Digital Empires* (Oxford University Press 2023).

frequently conceals deep normative and strategic fractures, as well as the existence of a regulatory pacing problem and asymmetric participation in standardisation. Ultimately, this situation raises the question of which kind of legal order can sustain effective regulation in an environment where competing governance models seek to project their norms globally.

IV. The Legitimacy Implications of the Paradigm Shift

16 As a result of the dynamics explored in the above-mentioned contributions to the special issue, it is clear that the role of technical standardisation in AI regulation goes beyond the regulatory setup which was established through the New Approach mechanism, acquiring more complex, multifaceted dimensions which have significant (geo-)political and ethical implications. This, in turn, entails unprecedented challenges for the existing mechanisms of accountability, eventually requiring a re-thinking of the way in which the European Commission and civil society interact with standardisation organisations.

17 In particular, **Mariolina Eliantonio** discusses the mechanisms and intensity of the control of the European Commission over harmonised standards, also in the light of the evolution of the case law and the practice of the European Commission. She argues that the Commission's control over draft standards represents the last crucial "public law check" in the European standardisation process, which the Commission ought to carry out with adequate depth. Going beyond mere rubber-stamping of draft standards prepared by ESOs is, in her view, both allowed and required by the Standardisation Regulation and the legislative setup foreseen by the New Legislative Framework. This control would prevent the transfer of indirect normative power to private actors - a risk all the more relevant in the framework of the AI Act where harmonised standards need to be controlled also for compliance with fundamental rights.

18 In the same perspective of improving the legitimacy of European standardisation activities, **Olia Kanevskaia** instead reflects on the existing instruments for securing that public interest is upheld in European standardisation, addressing the role of civil society and the issue of accessibility of technical standards for the public in this perspective. By discussing two key transparency challenges posed by the New Approach - i.e. access to standardisation processes and access to harmonised standards - the author argues that, although these issues are problematic at the European level, their resolution depends also on national institutions. In this sense, these issues pose compelling questions regarding the interplay between national and European accountability in the broader context of European standardisation policy, as well as the intentions and limits of the regulatory model adopted by the EU for pursuing a strong internal market that is based on the rule of law.

19 These reflections have become even more relevant today in the face of recent developments in the working method of JTC21. In order to accelerate the delivery of harmonised standards to support the AI Act, CEN and CENELEC have decided to allow, in the case of a positive "enquiry vote", direct publication of the drafts without a separate formal vote and to establish a small drafting group, composed of few experts, to finalise some standards.[42] This marks a "non-participatory turn", a stark reduction in transparency and stakeholder involvement compared to earlier standardisation efforts in adjacent regulatory domains, which calls for increased attention to the public and national avenues of control over standardisation processes.

V. Conclusions

20 The adoption of the AI Act represented a watershed moment in the EU governance of emerging technologies. At the heart of this regulatory architecture lies a reliance on technical standardisation that, while promising efficiency and agility, raises profound questions about the role of private actors in shaping public regulatory outcomes. The contributions to this special issue situate these technical instruments within broader ethical, legal, and geopolitical contexts. Whereas this practice is familiar in EU product safety regulation, it takes on new dimensions when applied to technologies with far-reaching implications for fundamental rights, democratic governance, and societal transformation. In particular, the presumption of conformity that the AI Act grants to harmonised standards, whereby compliance with such standards creates a rebuttable presumption of conformity with the Act's legal requirements, effectively delegates norm-setting authority to institutions whose decision-making procedures, composition, and accountability mechanisms differ markedly from those of public legislative and administrative bodies. As such, the standardisation of "risks" to fundamental rights forms an unprecedented delegation the task of protecting constitutional imperatives to private actors,[43] which exacerbates the long-standing issues of European standardisation and creates additional tensions with the EU legal system.

42 See https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/

43 See further Ho-Dac (n 33).

21 Still, the reliance on harmonised standards as a core compliance mechanism continues as a well-established trajectory in EU digital regulation, which was most recently reaffirmed in the Union's Data Strategy.[44] The promises of efficiency and agility of standardisation, however, are being concretely tested against the complex reality of AI regulation as a fast-paced and globally contended technology. Having entered into force in August 2024, the AI Act based the implementation of its rules concerning high-risk AI systems on the adoption of the relevant standards by 30 April 2025.[45] Following sensitive delays in the development of these standards by the ESOs, the deadline was first postponed to August 2025[46] and will probably extend into 2026.[47] Even more remarkably, the proposed Digital Omnibus on AI Regulation now puts forward that certain rules governing high-risk AI systems (Chapter III, Sections 1-3) would not enter into force until the Commission has adopted a corresponding decision confirming the existence of adequate support measures for the AI Act.[48] While these recent developments in the implementation of the AI Act confirm the crucial importance of harmonised standards for the functioning of this regulatory architecture, they also show actual limits in the speed and responsiveness to innovation of the current European standardisation ecosystem on which, *inter alia*, the European Commission intends to intervene.[49]

22 Moreover, the urgency in the adoption of these harmonised standards paved the way for worrisome recent changes in the process of standard-setting, in particular the decision to skip or compress certain stages of the standard-setting process,[50] specifically the deliberative ones, *de facto* leaving standard-setting power entirely in the hands of a small group of experts.[51] Shortly afterwards, the international standardisation organisations ISO and IEC decided to turn down the parallel development of two AI-related standards.[52] This development occurs against a backdrop of mounting tensions between European standardisation initiatives and international standard-setting processes, raising questions about regulatory fragmentation, technical interoperability, and the EU's broader aspirations for regulatory influence beyond its borders. Arguably, these issues cannot be divorced from broader geopolitical tensions, which have questions of digital regulation at their core.[53]

23 In the light of this, the aim of this special issue has been to reflect on the multifaceted implications of relying on technical standardisation in the context of the implementation of the AI Act, locating them in a broader context of ethical, legal and geopolitical issues, and examining the avenues for public control over these private activities. By exploring these dynamics, its ambition was to contribute to a broader emerging debate concerning the design and implementation of harmonised standards for AI systems and their intersection with fundamental rights protection, the legitimacy of EU decision-making processes, the trajectories of AI innovation and its limitations, and the contested terrain of European digital sovereignty. When private standardisation bodies develop technical specifications that effectively determine whether AI systems may lawfully process personal data, make

44 Communication from the Commission to the European Parliament and the Council data Union strategy unlocking data for AI, COM/2025/835 final, esp at 12.

45 Commission Implementing Decision of 22.5.2023 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, C(2023) 3215 final.

46 Commission Implementing Decision of 23.06.2025 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards high-risk AI-systems in support of Regulation (EU) 2024/1689 of the European Parliament and of the Council and repealing Implementing Decision C(2023)3215.

47 As reported in the press: Cynthia Kroet, 'EU standards bodies flag delays to work on AI Act' Euronews Next (16 April 2025) https://www.euronews.com/next/2025/04/16/eu-standards-bodies-flag-delays-to-work-on-ai-act accessed 2 March 2026.

48 Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM/2025/836 final.

49 European Commission, Call for evidence for an evaluation/fitness check, res(2023)5955298.

50 See https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/

51 See further on this point, Marta Cantero Gamito, 'From Consensus To Exceptionality – What The EU's AI Standards Crisis Reveals About Delegated Technical Governance', *(REALaw Blog, 28 November 2025).*

52 See https://www.mlex.com/mlex/articles/2403848/eu-ai-standard-setters-pause-of-consensus-process-has-international-fallout.

53 See further European Commission, *'Special Address by President Ursula von der Leyen: World Economic Forum Annual Meeting, Davos'* (Press Corner, European Commission, 19 January 2026) https://ec.europa.eu/commission/presscorner/detail/en/speech_26_150 accessed 2 March 2026 ("This reality also reflects the fact that Europe has all the assets it needs to attract investment – the savings, the skills, and the innovation – with our AI Factories and Gigafactories and the applications that are necessary, the 'AI first› principle. What we need is to mobilise collectively these assets to their full potential. And to focus on the essential. Focal point number one is to create a conducive and predictable regulatory environment".)

decisions affecting access to employment or social services, or shape the information environments within which citizens form opinions and exercise democratic rights, they are not regulating just a technical issue – it becomes a matter of how we want substantive rules to be adopted and the (digital) future of the EU to be shaped.

Decision Problems for Regulatees under the EU AI Act: Contested Values, Uncertain Evidence, and the Limits of Standardisation

by **Alessio Tartaro, Arvin Obnasca and Enrico Panai ***

Abstract: Based on the New Legislative Framework (NLF) approach, the AI Act relies on harmonised standards to provide technical specifications for the implementation of its essential requirements for high-risk AI systems. This paper argues that these requirements pose fundamental "decision problems" for regulatees, requiring value judgments and evidence assessment under uncertainty for their implementation. Unlike mature NLF fields with established methodologies and value consensus, the AI domain is characterised by contested values and uncertain evidence, significantly limiting the ability of traditional standardisation to provide clear, universally applicable solutions. This creates uncertainty for regulatees, complicates conformity assessment and enforcement, and risks undermining the overall regulatory effectiveness of the AI Act. In response to these challenges, this paper proposes supplementing standardisation with a procedural approach, such as documented "AI Act Compliance Cases," to compel transparent articulation and justification of regulatees' decisions. This enhances auditability and manageability, bolstering the Act's capacity to achieve its health, safety and fundamental rights objectives despite inherent complexities.

Keywords: AI Standardisation, AI Act, New Legislative Framework, AI Risks, Decision Problems

Recommended citation: Alessio Tartaro, Arvin Obnasca and Enrico Panai, Decision Problems for Regulatees under the EU AI Act: Contested Values, Uncertain Evidence, and the Limits of Standardisation, 17 (2026) JIPITEC 9 para 1.

I. Introduction

1 What constitutes an *acceptable level* of risk for AI systems? When is their *level of accuracy appropriate* for their intended purpose? What *measures of human oversight* are *commensurate* with the characteristics of an AI system, such as its level of autonomy and context of use? With the accelerating integration of AI into myriad aspects of private, social, and economic life, finding robust and actionable answers to these questions is becoming ever more pressing. Indeed, the ability to provide satisfactory responses to these questions may well mark the difference between AI that benefits society and AI that has a detrimental impact.

2 In this context, the AI Act has emerged as the first comprehensive legal framework specifically designed to regulate AI (superscript 1), in order to maximise its benefits and minimise its risks. Consequently, questions like those posed at the opening of this paper are not merely abstract philosophical

* Alessio Tartaro - University of Sassari, a.tartaro@phd.uniss.it
Arvin Obnasca - University of Sassari, a.obnasca@studenti.uniss.it
Enrico Panai - Catholic University of the Sacred Heart, enrico.panai@unicatt.it

1 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).

concerns but are central to the very fabric of the AI Act. They lie at the heart of the European vision of "Trustworthy and human-centric AI," an approach that explicitly aims to align the design, development, and deployment of AI technologies with established EU values and fundamental rights protection[2].

3 The primary burden of translating these high-level aspirations into concrete operational practice and demonstrating compliance with the Act's requirements falls squarely on the shoulders of regulatees, primarily providers of high-risk AI systems. For these actors, effectively navigating the AI Act requires addressing questions such as the acceptable level of risk (Article 9), the appropriate level of accuracy (Article 15), or the commensurability of human oversight measures (Article 14), in order to ensure compliance with the Regulation.

4 However, the AI Act itself does not provide direct, concrete answers to those questions. Regarding the level of risk, for instance, it merely states that the "overall residual risk of the high-risk AI systems is judged to be *acceptable*" (Article 9(5)). Concerning accuracy, Article 15(1) stipulates that "High-risk AI systems shall be designed and developed in such a way that they achieve an *appropriate level of accuracy*" and that "they perform consistently in those respects throughout their life cycle". On the crucial matter of human oversight, Article 14(1) mandates that "the oversight measures shall be *commensurate* with the risks, level of autonomy and context of the use of the high-risk AI system" (Article 14(1))[3]. This openness of the AI Act's core requirements generates significant interpretative, compliance, and enforcement uncertainty.

5 Since the AI Act relies on the New Legislative Framework (NLF)[4], a considerable expectation has arisen that these harmonised standards, developed by the European Standardisation Organisations (ESOs), will "come to the rescue" by providing the essential technical specifications and methodologies needed to concretise the Act's requirements[5]. This expectation is formally codified in the AI Act, where Article 40(1) confers a "presumption of conformity" on systems that comply with such standards. By making adherence to standards the principal means for providers to demonstrate that they meet the Act's legal obligations, the Regulation delegates a crucial role to the standardisation process, "kicking the can down the road" as a result[6]. This reliance on standards to bridge the gap between essential requirements and concrete technical implementation is a cornerstone of the NLF[7]. However, while this NLF model has proven successful in numerous other domains[8], this paper will argue that its application to the field of AI may not yield the anticipated effectiveness.

6 The core reason for this anticipated ineffectiveness lies in the nature of the questions regarding acceptable risk levels, appropriate accuracy levels, and commensurate human oversight measures, questions that regulatees are called upon to address with the support of harmonised standards. These problems can be effectively characterised as "decision problems", that is, problems requiring a choice between alternative courses of action, each with its own set of potential outcomes, benefits, and drawbacks[9]. For example, deciding an acceptable false positive rate for an AI system used in medical diagnosis requires balancing the risk of missing a condition against the risk of unnecessary delays in diagnosis, a choice influenced by varying clinical philosophies, resource constraints, and differing risk tolerance. Similarly, determining the "adequate" level of human oversight for an autonomous vehicle requires balancing the potential efficiency gains and convenience of automation against potential safety risks and the complex moral hazard considerations associated with shifting responsibility from human to machine. Such decisions depend heavily on prevailing societal values regarding safety, human agency, technological trust, and the

2 AI HLEG, 'Ethics Guidelines for Trustworthy AI' <https://ec.europa.eu/futurium/en/ai-alliance-consultation> accessed 4 March 2026.

3 Italics are ours.

4 Sybe de Vries, Olia Kanevskaia and Rik de Jager, 'Internal Market 3.0: The Old "New Approach" for Harmonising AI Regulation' (2023) 8 European Papers - A Journal on Law and Integration 583.

5 Josep Soler Garrido and others, 'Harmonised Standards for the European AI Act' (*JRC Publications Repository*, 2024) <https://publications.jrc.ec.europa.eu/repository/handle/JRC139430> accessed 27 May 2025.

6 Johann Laux, Sandra Wachter and Brent Mittelstadt, 'Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act' (2024) 53 Computer Law & Security Review 105957.

7 Stéphane du Boispéan, Markus Mueck and Christophe Gaie, 'Introduction to the European New Legislative Framework' in Markus Mueck and Christophe Gaie (eds), *European Digital Regulations* (Springer Nature Switzerland 2025) <https://doi.org/10.1007/978-3-031-80809-8_1> accessed 28 April 2025.

8 European Commission, 'Commission Staff Working Document: Evaluation of the New Legislative Framework' SWD(2022) 365 Final (16 November 2022) <https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12654-Industrial-products-evaluation-of-the-new-legislative-framework_en> accessed 18 February 2026.

9 B Fischhoff and others, 'Approaches to Acceptable Risk: A Critical Guide' (1980) NUREG/CR-1614, ORNL/Sub-7656/1, 5045395 <http://www.osti.gov/servlets/purl/5045395/> accessed 6 November 2024.

acceptability of different types of errors. For high-risk AI systems listed in Annex III of the AI Act, the ultimate determination of compliance, including judgments about "acceptable risk" or "appropriate accuracy," rests with the regulatees, primarily AI providers themselves, through internal conformity assessment. For high-risk AI systems referred to in Annex I (i.e., products or safety components of products covered by sectoral legislation), this judgment will often involve notified bodies[10]. Successfully addressing these decision problems is therefore a key element for all regulatees aiming to achieve and demonstrate compliance with the AI Act, for competent authorities enforcing it and for notified bodies assessing conformity.

7 An essential characteristic of such decision problems is their inherent dependence on two intertwined factors: values (what is considered desirable or undesirable, important or trivial) and evidence (information about the likely outcomes of different choices)[11]. In other words, a combination of (often implicit) value judgments and available empirical evidence influences the choice between the different alternatives that define any given decision problem. In the rapidly evolving field of AI, however, a critical complicating factor emerges: the relevant values are frequently contested, pluralistic, and subject to ongoing societal debate (constituting an ethical problem)[12], and the evidence regarding AI system performance, reliability, and broader societal impact is often weak, incomplete, uncertain, or context-dependent (constituting an epistemological problem)[13]. This combination presents a significant obstacle to defining a common, universally accepted way of handling these decision problems in the AI domain, particularly for regulatees seeking clear, predictable, and defensible pathways to compliance.

8 As we shall see, this situation contrasts sharply with decision problems in many other, more mature fields regulated under the NLF. In those sectors, although values and uncertainty invariably play a role, commonly accepted methods, data collection and evaluation practices, and established professional norms are often codified into harmonised standards to guide the identification of the most acceptable alternative and thus finding a broadly satisfactory solution to the decision problem at hand. This disparity has direct and profound implications for what standards can realistically achieve in supporting the implementation of the AI Act, calling into question the anticipated role of harmonised standards in facilitating compliance and supporting the achievement of the Regulation's ambitious objectives.

9 The remainder of this paper will develop arguments to support these claims. While acknowledging the extensive literature already emerging on the AI Act and the role of standards showcased in this special issue, this paper focuses specifically on the "decision problems" faced by regulatees. Section 2 will elaborate on the nature of decision problems and demonstrate how many of the essential requirements for high-risk AI systems are indeed of this type, posing direct and often underappreciated challenges for regulatees. Section 3 will then delve deeper into why these decision problems are particularly difficult to handle in the field of AI, highlighting the pervasive divergences in values and the inherent uncertainty of evidence that characterise this domain, illustrated with a use case. Section 4 will further underscore these challenges by contrasting the AI context with other NLF-regulated fields where decision problems, while present, are often more robustly addressed by standards due to greater epistemic and normative consensus. Section 5 will examine the regulatory implications of these limitations for the AI Act and propose a procedural documentation structure, similar to assurance cases, and clarified roles of technical standards to manage inherent decision problems.

10 See Irene Kamara's paper in this special issue.

11 Baruch Fischhoff, 'Acceptable Risk: A Conceptual Proposal' (1994) 5 RISK: Health, Safety & Environment (1990-2002) <https://scholars.unh.edu/risk/vol5/iss1/3>.

12 Catharina Rudschies, Ingrid Schneider and Judith Simon, 'Value Pluralism in the AI Ethics Debate – Different Actors, Different Priorities' (2020) 29 The International Review of Information Ethics <https://informationethics.ca/index.php/irie/article/view/419> accessed 30 May 2025.

13 Rishi Bommasani and others, 'A Path for Science- and Evidence-Based AI Policy' <https://understanding-ai-safety.org/> accessed 27 March 2026.

II. Essential Requirements and Decision Problems in the AI Act

10 In line with the NLF underpinning its structure[14], the AI Act articulates essential requirements for high-risk AI systems and delegates their technical elaboration to harmonised standards[15], which Article 40 regards as providing a presumption of conformity[16]. These essential requirements are outlined in Articles 8 to 15 of Title III, Chapter 2, which include high-quality data and data governance, comprehensive technical documentation, robust record-keeping, transparency and provision of clear information, effective human oversight mechanisms, and appropriate levels of accuracy, robustness, and cybersecurity. Article 9 is particularly important because it requires a continuous, iterative risk management strategy throughout the entire life cycle. The other requirements in Articles 10 to 15 can be understood as particular risk mitigation measures within the broader framework. The regulatory reasoning, therefore, shifts from isolated technical compliance to organised risk governance. Its ultimate goal is that any residual risks, after all reasonable protections have been implemented, be deemed "acceptable" in line with Article 9(5)[17].

11 Viewed through this analytical lens, it becomes evident that implementing the AI Act's requirements to achieve and demonstrate conformity invariably confronts providers with a series of complex decision problems. Indeed, determinations of risk acceptability are, by their very nature, archetypal decision problems[18]. Such problems necessitate choices among various alternative courses of action, each associated with distinct potential outcomes, benefits, harms, and inherent uncertainties. From this standpoint, an "acceptable risk" is not an objective, pre-existing quantity but rather the outcome associated with the most preferable alternative identified within a specific decision problem, after considering all relevant factors, including societal values, technical feasibility, economic implications, available evidence, and ethical considerations.

12 Consider, for instance, the development of an AI system used in autonomous vehicles, a high-risk application under Annex I. A regulatee (the AI provider) must decide on the trade-offs inherent in its design and performance. Providers must grapple with unavoidable accident scenarios (the "trolley problem" in a new guise)[19]. Should the system be programmed to prioritise the safety of its occupants above all else, or to minimise the total number of potential casualties, even if this entails a greater risk to those within the vehicle? This is a profound ethical decision problem with no single "correct" answer. A further example arises with AI systems intended for content moderation on large online platforms, which, even if they don't fall under the AI Act's high-risk categories, remain highly relevant due to their intersection with the Digital Services Act[20]. Is it more "acceptable" to implement highly aggressive filtering algorithms for potentially harmful content, thereby risking the erroneous removal of legitimate expression and impinging on freedom of speech (a false positive)? Or is it preferable to adopt a more lenient approach that, while safeguarding free speech more broadly, risks the wider proliferation of harmful material, hate speech, or disinformation (a false negative)? These illustrative scenarios underscore the challenging, value-laden trade-offs inherent in determining "acceptable risk" or "appropriate" accuracy, where

14 See, in particular, Article 3 of Decision No 768/2008/EC, according to which, for legislation concerning the marking of products, "Community harmonisation legislation shall restrict itself to setting out the essential requirements determining the level of such protection and shall express those requirements in terms of the results to be achieved," and further, that "where Community harmonisation legislation sets out essential requirements, it shall provide for recourse to be had to harmonised standards, adopted in accordance with Directive 98/34/EC, which shall express those requirements in technical terms."

15 This division of responsibilities, whereby essential requirements are articulated in legislation as high-level objectives, and technical standards, developed by the ESOs, provide detailed technical specifications, forms a foundational principle of European product safety legislation. See, for example, Jacques Pelkmans, 'The New Approach to Technical Harmonization and Standardization' (1987) 25 JCMS: Journal of Common Market Studies 249.

16 Mark McFadden and others, 'Harmonising Artificial Intelligence: The Role of Standards in the EU AI Regulation' <https://oxil.uk/publications/2021-12-02-oxford-internet-institute-oxil-harmonising-ai/> accessed 11 March 2026; Alessio Tartaro, 'Regulating by Standards: Current Progress and Main Challenges in the Standardisation of Artificial Intelligence in Support of the AI Act' [2023] European Journal of Privacy Law & Technologies.

17 Jonas Schuett, 'Risk Management in the Artificial Intelligence Act' [2023] European Journal of Risk Regulation 1; Henry Fraser and José-Miguel Bello y Villarino, 'Acceptable Risks in Europe's Proposed AI Act: Reasonableness and Other Principles for Deciding How Much Risk Management Is Enough' [2023] European Journal of Risk Regulation 1.

18 Fischhoff and others (n 9).

19 Norbert Paulo, 'The Trolley Problem in the Ethics of Autonomous Vehicles' (2023) 73 The Philosophical Quarterly 1046.

20 Paddy Leerssen, 'An End to Shadow Banning? Transparency Rights in the Digital Services Act between Content Moderation and Curation' (2023) 48 Computer Law & Security Review 105790.

straightforward, universally agreed-upon, or purely technical solutions are often elusive. Regulatees are thus forced to make difficult judgments, balancing competing objectives and values on the basis of uncertain evidence. Even requirements that appear more technical, such as "sufficiently representative" training data (Article 10), resolve into decision problems for regulatees. What constitutes "sufficiently representative" training data to avoid harmful bias related, for example, to different performance for different demographic groups[21]? The regulatee must decide on the relevant demographic categories, the acceptable thresholds for representation within each, and the methods for measuring and mitigating identified biases[22]. These are not purely technical questions; they involve value judgments about fairness, equity, and the potential consequences of data-driven discrimination.

13 How, then, are such choices among competing alternatives in these decision problems to be made by regulatees in a manner that is defensible, transparent, and compliant with the AI Act's spirit? While the AI Act appears to assign a fundamental role to harmonised standards in this context, the current state of techno-scientific development in the field of AI, characterised fundamentally by contested values and uncertain evidence, makes the codification of unambiguous answers to these crucial questions within harmonised standards truly improbable. The next two sections will provide support for this argument.

III. Contested Values and Uncertain Evidence in the Field of AI

14 While Article 40 is intended to provide a clear compliance pathway via harmonised standards, we argue that the practical application of the essential requirements for high-risk AI systems under the AI Act still necessitates that regulatees navigate a series of complex decision problems which involve contested values and uncertain evidence. To show this, we will proceed by examining a plausible, albeit hypothetical, case study. This illustrative approach will allow us to demonstrate why neither the AI Act's legislative text nor, in all likelihood, the forthcoming harmonised standards can currently provide straightforward, unambiguous, or universally applicable solutions to these deep-seated challenges.

15 Consider the hypothetical case of "DoctorLLM," a sophisticated software system based on a large language model (LLM). This system is designed to process natural language questions and inputs from physicians and other qualified medical personnel. In response, it generates natural language outputs intended to provide recommendations concerning the diagnosis, treatment, or monitoring of human diseases and health conditions. Given its intended purpose, i.e., to provide information used to make decisions with diagnostic or therapeutic purposes, this system clearly falls under the purview of the MDR. According to Annex VIII, Section 6.3, Rule 11 of the MDR, software intended to provide information which is used to make decisions for diagnosis or therapeutic purposes is classified as at least Class IIa. It could be classified as Class IIb or even Class III depending on whether these decisions have an impact that may cause a serious deterioration of a person's state of health or a surgical intervention, or death or an irreversible deterioration of a person's state of health, respectively. For the sake of simplicity, let us assume, for this scenario, that DoctorLLM is classified just as Class IIa under the MDR, which requires challenging third-party conformity assessment[23]. Furthermore, this system would unequivocally be qualified as a high-risk AI system under the AI Act by virtue of Article 6(1a) as it is a product, i.e., a software as medical device, covered by the MDR, which is included in Annex I. Consequently, the provider of DoctorLLM, our regulatee, must ensure compliance not only with the stringent requirements of the MDR but also with all the applicable essential requirements stipulated by the AI Act and applicable to high-risk AI systems.

16 As mentioned, among these AI Act requirements, Article 9 mandates the implementation of a robust and continuous risk management system to ensure that "the overall residual risk of the high-risk AI system is judged to be acceptable." Another pivotal essential requirement, detailed in Article 15, stipulates that DoctorLLM must be designed and developed to achieve a level of accuracy, robustness, and cybersecurity that is "appropriate" to its intended purpose and context of use[24].

21 Laleh Seyyed-Kalantari and others, 'Underdiagnosis Bias of Artificial Intelligence Algorithms Applied to Chest Radiographs in Under-Served Patient Populations' (2021) 27 Nature Medicine 2176.

22 Line H Clemmensen and Rune D Kjærsgaard, 'Data Representativity for Machine Learning and AI Systems' (arXiv, 3 February 2023) <http://arxiv.org/abs/2203.04706> accessed 5 June 2024; FF Liza, 'Challenges of Enforcing Regulations in Artificial Intelligence Act - Analyzing Quantity Requirement in Data and Data Governance' (2022) <https://ceur-ws.org/Vol-3221/IAIL_paper9.pdf> accessed 21 February 2026.

23 Tuomas Granlund, Tommi Mikkonen and Vlad Stirbu, 'On Medical Device Software CE Compliance and Conformity Assessment', *2020 IEEE International Conference on Software Architecture Companion (ICSA-C)* (2020) <https://ieeexplore.ieee.org/abstract/document/9095660> accessed 30 May 2025.

24 Here, 'accuracy' can be broadly understood as functional correctness and reliability in generating clinically relevant

However, determining precisely what constitutes an "acceptable" level of overall residual risk or an "appropriate" level of accuracy for a system like DoctorLLM presents profound and multifaceted challenges for the regulatee. These are quintessential decision problems, characterised by contested values and uncertain evidence.

17 Establishing what constitutes an "acceptable" level of risk for a system such as DoctorLLM is particularly complex. It is not merely a technical calculation but a judgment that must balance the severity and probability of potential harms—such as misdiagnoses, inappropriate treatments, or the erosion of trust in the healthcare system—against the expected benefits. This evaluation is inherently subjective, influenced by ethical values, and made even more daunting by epistemic uncertainties about the system's actual ability to operate safely across all varied and unpredictable real-world clinical contexts, as well as the difficulty of anticipating every possible failure mode or misuse of the system. Furthermore, the definition of "acceptable" can vary significantly depending on the perspectives of the stakeholders involved (patients, physicians, healthcare institutions, and society at large), making consensus an elusive goal.

18 At first glance, problems concerning the determination of an "appropriate level of accuracy" for DoctorLLM might appear somewhat less structurally complex than those involving "overall risk acceptability." Nevertheless, they too rest fundamentally on underlying value judgments and assessments of uncertain evidence, which the regulatee must carefully consider. Determining the appropriate level of accuracy for DoctorLLM is not just about achieving the highest possible number in isolation; it involves defining a performance standard that is clinically safe and sufficient for its intended use case, balancing different types of potential errors (e.g., false positives vs. false negatives) based on the severity of the condition and the consequences of misdiagnosis.

19 Furthermore, determining the "acceptability of the evidence" that supports claims about a given level of accuracy is itself a critical and often overlooked part of this decision problem. This relates closely to what philosophers of science have termed "inductive risk", i.e., the risk of error inherent in making inductive inferences from limited evidence, and the value judgments involved in deciding how much evidence is "sufficient" to accept or reject a hypothesis[25]. Ascertaining the true, generalisable accuracy of a complex AI system like DoctorLLM is fraught with challenges for the regulatee. These challenges include limitations in the validation datasets used to test the system (e.g., representativeness, bias), questions about potential performance degradation or "drift" over time as medical knowledge and patient populations evolve, and the inherent difficulty in translating accuracy demonstrated in controlled lab settings to the complex, varied environment of real-world clinical practice. Additionally, there is epistemic uncertainty about the model's behaviour across the full range of potential inputs, particularly regarding novel or edge cases and the risk of generating inaccurate information, commonly known as "hallucinations."

IV. Addressing Decision Problems in NLF-regulated Fields

20 Upon closer inspection, the situation described above, where essential legislative requirements are articulated in broad, outcome-oriented terms, and the detailed technical means for achieving compliance are expected to be provided by harmonised standards, does not appear, on the surface, to be fundamentally different from that encountered in several other well-established fields regulated under the NLF. Precisely because NLF legislation is designed to delegate the specification of technical means for implementing the delineated essential requirements to standardisation bodies, these essential requirements are, by necessity, often couched in somewhat vague or general terms within the legislative text itself. Even in mature NLF sectors such as toys, machinery, or medical devices, regulatees (manufacturers and other economic operators) are continuously confronted with decision problems analogous to those described for AI regulatees.

21 For instance, how does a manufacturer of a high-risk medical device (a regulatee under the MDR) determine that, as an outcome of their comprehensive risk management process, "the residual risk associated with each hazard as well as the overall residual risk is judged acceptable," as mandated by Annex I, Chapter 1, Point 4 of the MDR? This problem of judging risk acceptability is structurally very similar to the challenge concerning the acceptability of risk for high-risk AI systems (Article 9(5) AI Act) faced by AI regulatees like the provider of DoctorLLM. Both involve making a judgment call about safety and risk in the face of uncertainty.

22 There is, however, a crucial set of differences between these established NLF fields and the nascent domain of AI regulation that significantly impacts how regulatees can approach and resolve these inherent decision problems. These differences relate fundamentally to the maturity of the field,

and sound recommendations.

25 Heather Douglas, 'Inductive Risk and Values in Science' (2000) 67 Philosophy of Science 559.

the availability of methodologies for evidence generation and evaluation, and the degree of societal and professional consensus on underlying values and acceptable trade-offs.

23 In contrast to the often-uncharted territory of AI, decisions regarding the acceptability of risk for a traditional medical device, for example, are typically conducted according to rigorous, systematic, and internationally recognised procedures. A cornerstone of this process is clinical investigation and evaluation. Clinical investigations for medical devices are conducted in line with widely accepted and highly detailed international standards, most notably ISO 14155:2020 on "Clinical investigation of medical devices for human subjects – Good clinical practice." This standard, and others like it, provide a comprehensive framework for the systematic and controlled collection of clinical data. During this process, the safety and performance of a medical device can be quantitatively measured through shared, validated, and meticulously documented testing procedures, patient follow-up, and statistical analysis. This ability to generate evidence systematically and rigorously, using methods that are themselves subject to consensus and standardisation, constitutes the first, crucial epistemic element that differentiates established NLF cases like medical devices from the current state of affairs in AI. Such established methodologies provide much clearer pathways for regulatees in those traditional sectors to gather the evidence needed to support their resolution of these decision problems in order to show compliance.

24 Yet, this systematic evidence collection and evaluation, while vital, is only the first differentiating element. As discussed, any collection, interpretation, and application of evidence is also subject to underlying value choices. Philosopher Heather Douglas has compellingly articulated the concept of "inductive risk," which refers to the unavoidable role of non-epistemic (e.g., ethical, social, economic) values in scientific judgment, particularly when deciding how much evidence is sufficient to accept or reject a scientific claim, and in weighing the potential societal consequences of being wrong (e.g., the cost of a false positive versus a false negative in a regulatory context)[26]. This involves value-laden decisions about what constitutes valid evidence, how it should be collected and interpreted, what level of uncertainty is tolerable, and at what point investigation can reasonably cease, balancing the pursuit of greater certainty against practical constraints and societal needs.

25 Crucially, in the field of AI, these fundamental value-laden decisions regarding evidence generation, interpretation, and the thresholds for acceptability are often as contested and unsettled as the empirical evidence itself, creating significant ambiguity and burden for regulatees. This is partly because, as acknowledged in the European Commission in the impact assessment accompanying the proposed AI Act, "robust and representative evidence for harms inflicted by the use of AI is scarce due to lack of data and mechanisms to monitor AI as a set of emerging technology"[27]. Under the stringent criteria for evidence-based policymaking and risk assessment typically applied in established domains such as pharmaceutical regulation or environmental risk assessment[28], such an acknowledged scarcity of robust, longitudinal evidence might have raised significant questions about the sufficiency of the evidentiary basis for a comprehensive legislative intervention of the AI Act's scale. This divergence arguably highlights a difference in underlying values guiding the regulatory approach itself: in the AI context, pressing concerns about the potential future threats posed by AI to fundamental rights, democratic values, rule of law, and societal well-being appear to have (perhaps justifiably) prevailed over strict adherence to the rigorous, data-intensive criteria for evidence collection, evaluation, and validation that might be demanded before similar evidence-based regulatory action in other, more data-rich areas[29]. While this proactive stance may be commendable from a precautionary perspective, it leaves AI regulatees to navigate a complex regulatory landscape with far fewer established evidential benchmarks and a less developed societal consensus on how to weigh competing values.

26 Unlike in the field of AI, in mature NLF domains such as medical devices, toys or machinery safety, decision problems regarding risk acceptability and other evidence-based and value-laden problems can often be resolved by regulatees in a shared, relatively uncontested, and predictable manner. This predictability in mature fields is grounded in a convergence of shared epistemic foundations, enabled by validated methodologies for systematic evidence generation, and a higher degree of societal and professional consensus on underlying values, including what constitutes acceptable risk levels

26 Douglas (n 26).

27 'Impact Assessment of the Regulation on Artificial Intelligence' (Shaping Europe's Digital Future, 21 April 2021) <https://digital-strategy.ec.europa.eu/en/library/impact-assessment-regulation-artificial-intelligence> accessed 3 August 2023.

28 Špela Majcen, 'Evidence Based Policy Making in the European Union: The Role of the Scientific Community' (2017) 24 Environmental Science and Pollution Research 7869.

29 Stephen Casper, David Krueger and Dylan Hadfield-Menell, 'Pitfalls of Evidence-Based AI Policy' (arXiv, 18 April 2025) <http://arxiv.org/abs/2502.09618> accessed 30 May 2025.

and the core principles guiding necessary trade-offs. Technical standards in these sectors effectively codify these shared understandings, translating agreed-upon methods for evidence generation and established criteria for interpreting that evidence into practical guidance that facilitates compliance for regulatees. In contrast, the AI domain currently lacks this robust foundation of shared methodologies and value consensus, which consequently renders the codification of these elements into harmonised standards exceedingly challenging at present.

V. Implications and Potential Solutions

27 This inherent difficulty in translating the AI Act's high-level, often deliberately vague, essential requirements into concrete, readily implementable, and consistently verifiable specifications for providers constitutes a significant hurdle for their compliance efforts and, by extension, for the overall success of the Act[30].

28 A principal implication of this potential misalignment between the NLF's assumptions and the realities of AI governance is the risk of undermining the regulatory effectiveness of the AI Act[31]. In this context, regulatory effectiveness can be understood as the capacity of a regulatory regime to achieve its stated objectives[32], i.e., in the case of the AI Act, ensuring a high level of protection for health, safety, and fundamental rights, fostering legal certainty, promoting innovation, and building public trust in AI. If the core "decision problems" that lie at the heart of the AI Act cannot be robustly and consistently addressed by regulatees through the anticipated guidance of harmonised standards, due to the aforementioned deep-seated challenges with divergent values and uncertain evidence, then the burden of interpretation and practical implementation shifts significantly, and often problematically, onto these individual economic actors.

29 Secondly, without clear, widely accepted benchmarks derived from such standards, conformity assessment procedures, either conducted via internal control for Annex III systems or involving notified bodies for Annex I systems, may lack consistency, comparability, and, in some cases, sufficient rigour. This, in turn, could significantly hamper the oversight capacity and effectiveness of notified bodies[33] (where involved) and national competent authorities. If each regulatee develops idiosyncratic interpretations of "acceptable risk" or "appropriate accuracy," or if different notified bodies apply varying criteria, the goal of a harmonised level of protection and a level playing field across the EU internal market could be jeopardised. Different Member States might also see their national authorities adopt divergent enforcement stances based on their own interpretations of these open-textured terms, leading to regulatory fragmentation rather than harmonisation. This is a particular concern for small and medium-sized enterprises, which constitute a significant portion of the AI development landscape in Europe, but may lack the extensive legal and technical resources of larger corporations to navigate such profound ambiguities and develop bespoke, highly sophisticated internal governance processes for each decision problem.

30 Consequently, the Act's ability to genuinely mitigate risks and protect fundamental rights in a consistent and predictable manner could be diluted, thereby impeding the achievement of its core societal goals. The actions, interpretations, and internal decision-making processes of regulatees are thus absolutely critical to the overall regulatory effectiveness of the AI Act. Where these regulatees face undue ambiguity, intractable value conflicts without clear guidance, or insurmountable evidential burdens, the effectiveness of the entire regulatory edifice suffers[34]. The promise of "presumption of conformity" via harmonised standards, a key pillar of the NLF[35], may prove illusory or difficult to attain in practice for many core AI Act requirements if the harmonised standards themselves cannot adequately capture and resolve these underlying decision problems.

30 Alessio Tartaro, 'Towards European Standards Supporting the AI Act: Alignment Challenges on the Path to Trustworthy AI.', *Proceedings of the AISB Convention 2023* (2023) <https://ssrn.com/abstract=4470766>.

31 Alessio Tartaro, 'Value-Laden Challenges for Technical Standards Supporting Regulation in the Field of AI' (2024) 26 Ethics and Information Technology 72.

32 Morag Goodwin and Roger Brownsword (eds), 'Regulatory Effectiveness I', *Law and the Technologies of the Twenty-First Century: Text and Materials* (Cambridge University Press 2012) <https://www.cambridge.org/core/books/law-and-the-technologies-of-the-twentyfirst-century/regulatory-effectiveness-i/F8062987DBCD0CE416B062C31FB7B992> accessed 30 May 2025.

33 See the contribution of Kamara and others in this special issue.

34 Morag Goodwin and Roger Brownsword (eds), 'Regulatory Effectiveness III: Resistance by Regulatees', *Law and the Technologies of the Twenty-First Century: Text and Materials* (Cambridge University Press 2012) <https://www.cambridge.org/core/books/law-and-the-technologies-of-the-twentyfirst-century/regulatory-effectiveness-iii-resistance-by-regulatees/418FCE986492BF2447F589AD61102678> accessed 30 May 2025.

35 Philippe Portalier, 'Myths and Realities of the Presumption of Conformity' <https://orgalim.eu/insights/myths-and-reality-presumption-conformity> accessed 6 April 2026.

31 To address the profound difficulties in operationalising the AI Act's essential requirements for high-risk systems, the solution proposed in the rest of this section aims to bolster the procedural and evidentiary foundation of conformity assessments, compelling regulatees to transparently articulate how they have navigated these complex decision problems, thereby shifting some emphasis from elusive substantive harmonisation via standards to robust procedural harmonisation and documented reasoning. Instead of relying solely on standards to deliver substantive solutions, a complementary approach that focuses on procedural rigour and transparency in regulatees' decision-making processes offers a more promising path forward. This approach aims to make the internal deliberation processes for these decision problems more manageable for regulatees and, consequently, more transparent and auditable for notified bodies and competent authorities.

32 Given the recent debate on the potential revision of the AI Act[36], the core proposal here involves amending the documentation requirements in Article 11 and Annex IV of the AI Act to explicitly require providers of high-risk AI systems to develop, document, and maintain what can be termed an "AI Act Compliance Case." This concept draws inspiration from established practices of "safety cases" in critical industries (e.g., aviation, nuclear power, railway signalling) and "assurance cases" increasingly discussed in the context of AI safety and ethics[37]. An "AI Act Compliance Case" would be a structured body of evidence and argumentation, forming a central part of the technical documentation, that explicitly demonstrates how the regulatee has identified, analysed, deliberated upon, and resolved the key decision problems pertinent to their specific high-risk AI system in order to meet the Act's essential requirements.

33 Specifically, this enhanced documentation would mandate that regulatees (primarily providers, but with implications for deployers who may need to contribute or verify parts of it) undertake and record the following:

34 Identification and framing of decision problems: regulatees would be required to explicitly identify the specific decision problems they encountered in seeking to comply with each relevant essential requirement. This includes articulating the alternatives considered and the core trade-offs involved for their particular AI system and its intended context of use.

35 Articulation of relevant values: For each significant decision problem, the regulatee must document the relevant values that were considered pertinent. This involves acknowledging potential conflicts between these values. Standards such as the IEEE 7000 offer a structured process to carry out these activities[38], and dedicated professionals can support the process[39].

36 Evidential basis and uncertainty assessment: The regulatee must comprehensively outline the evidential basis used to inform their decisions. This includes detailing the data, metrics, testing methodologies, and validation processes employed to generate evidence regarding the system's performance, reliability, and potential impacts. Crucially, this section must also include a transparent assessment of the limitations, uncertainties, and potential biases inherent in this evidence (e.g., gaps in training data, limitations of testing environments, and generalisability concerns).

37 Deliberation and justification of trade-offs: Given that many "decision problems" in AI involve balancing competing concerns, regulatees must provide a thorough explanation of how trade-offs between potentially conflicting values or objectives were deliberated upon and ultimately resolved. This would require them to document the decision-making process, the alternatives considered, the rationale for the chosen approach, and a robust justification for why this approach is deemed to lead to compliance with the AI Act (e.g., achieving an "acceptable" risk level or "appropriate" accuracy) in light of the system's intended purpose, context of use, and the acknowledged values and evidence.

38 While this proposal undoubtedly introduces a significant documentation requirement, it aims to make the underlying decision problems more manageable for regulatees in several ways,

36 'EU Commission Opens Door for "Targeted Changes" to AI Act' (POLITICO) <https://www.politico.eu/article/gpai-code-of-practice-to-come-in-weeks-ai-office-says/> accessed 30 May 2025.

37 Rasmus Adler and Michael Klaes, 'Assurance Cases as Foundation Stone for Auditing AI-Enabled and Autonomous Systems: Workshop Results and Political Recommendations for Action from the ExamAI Project' in Matthias Rauterberg and others (eds), *HCI International 2022 – Late Breaking Papers: HCI for Today's Community and Economy*, vol 13520 (Springer Nature Switzerland 2022) <https://link.springer.com/10.1007/978-3-031-18158-0_21> accessed 5 November 2023.

38 IEEE, 'IEEE Std 7000™-2021. IEEE Standard Model Process for Addressing Ethical Concerns during System Design' <https://standards.ieee.org/ieee/7000/6781/>; Sarah Spiekermann, 'From Value-Lists to Value-Based Engineering with IEEE 7000™', *2021 IEEE International Symposium on Technology and Society (ISTAS)* (IEEE 2021) <https://ieeexplore.ieee.org/document/9629134/> accessed 6 June 2022.

39 Mariangela Zoe Cocchiaro and others, 'Who Is an AI Ethicist? An Empirical Study of Expertise, Skills, and Profiles to Build a Competency Framework' [2025] AI and Ethics <https://doi.org/10.1007/s43681-024-00643-y> accessed 2 June 2025.

rather than simply adding to their burden. The proposed approach aims to enhance manageability for regulatees by providing a clear, structured framework for tackling complex, ill-defined problems, thereby replacing vague requirements with a defined process of analysis and justification. It shifts the focus from searching for elusive "correct" answers to developing robust, evidence-informed justifications for choices, which is often more achievable and fosters better internal understanding and risk management within the regulatees' organisation. This method also offers procedural certainty on how to demonstrate due diligence, even if substantive uncertainty about acceptable risk persists. In this revised framework, harmonised standards still play a crucial, though reoriented, role by supporting the process of reasoned justification rather than dictating specific outcomes. Standards could define the structure and methodology for preparing Compliance Cases, specify accepted methods for generating evidence, like bias testing, propose common metrics, or offer sector-specific guidance for typical decision problems. However, the ultimate judgment, documented in the Compliance Case, would remain with the regulatee, subject to assessment by conformity bodies and enforcement by competent authorities whenever appropriate. This, in turn, would bolster the AI Act's overall regulatory effectiveness by empowering regulatees with a clearer and more manageable framework for demonstrating compliance, facilitating more effective and consistent oversight, and fostering a culture of responsible AI development and deployment. It moves the AI Act towards a model where compliance is demonstrated not just by ticking boxes against standards, but by providing a compelling, evidence-backed narrative of due diligence and reasoned judgment in the face of inherent complexity.

39 However, it is crucial to acknowledge that this proposed shift from substantive, standards-based conformity to procedural, argument-based compliance presents its own challenges, particularly for the controlling authorities. The evaluation of a bespoke compliance case is inherently more resource-intensive and time-consuming than verifying conformity with a harmonised standard. Unlike a technical specification, a compliance case is a qualitative argument about navigating trade-offs and values. Its adequacy is not a matter of objective measurement but of reasoned judgment, making the assessment process itself inherently contestable. Each case would require deep, bespoke analysis by competent authorities, potentially leading to regulatory bottlenecks. The very process designed to enhance transparency for regulatees could therefore become a source of profound practical strain and disagreement for the authorities tasked with its assessment.

40 Nevertheless, this challenge does not invalidate the proposal; rather, it exposes the true and unavoidable cost of effectively regulating artificial intelligence. The strain on authorities is not a flaw in the compliance case model but a symptom of the inherent complexity of AI governance—a complexity that the standard-centric approach merely obscures rather than solves. Relying solely on standards risks creating a veneer of simplicity over a reality of inconsistent application and superficial compliance. The compliance case, by contrast, forces this difficult and resource-intensive work into a documented, auditable, and transparent format. The resulting political and financial challenge of equipping authorities to handle these assessments is therefore not a reason to retreat to a failing model, but an essential precondition for the AI Act to achieve its stated goals. In essence, it trades the false comfort of a simple but ineffective process for the demanding reality of a complex but ultimately more robust regulatory regime.

VI. Conclusion

41 This paper has explored the fundamental challenge posed by the AI Act's approach to regulating high-risk AI systems, specifically how its reliance on the NLF confronts significant friction points when applied to the inherent nature of several core essential requirements. We have argued that requirements such as ensuring "acceptable risk," "appropriate accuracy," and "commensurate human oversight" do not readily lend themselves to straightforward, universally applicable technical specifications capable of being fully codified within harmonised standards. Instead, these requirements compel us to grapple with intricate "decision problems" that necessitate balancing competing values and making judgments in the face of often profound epistemic uncertainty.

42 In contrast to sectors with established, widely accepted methodologies for systematic evidence generation and a higher degree of consensus on the values guiding the interpretation of that evidence and the determination of acceptable thresholds, the field of AI currently presents a landscape marked by divergent values, uncertain and evolving evidence, and a lack of established benchmarks for navigating complex trade-offs. While standards in mature domains can effectively codify shared epistemic and normative understandings into practical compliance guidance, the same mechanism faces substantial limitations in fully addressing the deep-seated value conflicts and pervasive uncertainties inherent in many AI applications.

43 The significant implication of this divergence is the potential diminishment of the AI Act's regulatory

effectiveness. In light of these challenges, this paper has finally proposed a complementary approach focused on enhancing the procedural rigour and transparency of regulatees' internal decision-making processes. The concept of an "AI Act Compliance Case," drawing inspiration from established safety and assurance case methodologies, serves as the cornerstone of this proposal. Within this proposal, harmonised standards would retain a crucial, albeit reoriented, role: supporting the process of reasoned justification by defining methodologies for evidence generation, structuring compliance documentation, and providing guidance on specific aspects, rather than attempting to provide definitive substantive answers to value-laden decision problems.

44 Ultimately, navigating the inherent complexities of AI governance requires moving beyond the sole expectation of static technical standards providing all the answers. By fostering a culture of transparent, accountable decision-making encapsulated in Compliance Cases, the AI Act can more effectively translate its high-level aspirations into concrete, verifiable, and trustworthy AI systems that genuinely benefit society while upholding fundamental rights and Union values.

From National to European - And Back Again: Fixing the Flaws of the New Approach

by **Olia Kanevskaia** *

Abstract: Harmonized standards are central to European policymaking. Traditionally intended to ensure technical harmonization and consumer safety, harmonized standards are increasingly becoming critical for regulating many societal aspects: to illustrate, the recently adopted AI Act outsources many legal and ethical decisions to the European standards bodies. In this setting, questions whether and how public interest is sufficiently safeguarded in the private setting of European standardizations are bound to arise.

Developed mainly by commercial actors, harmonized standards are under little – if any – control of civil society. Firstly, participation of societal stakeholders in technical standardization processes remains limited; secondly, despite the recent jurisprudence, access to harmonized standards remains challenging. Academic and policy discussions on these issues abound; however, the role of Member States, and more specifically National Standards Organizations in ensuring participation in and access to standards, tends to be sidestepped.

This paper examines two key transparency challenges posed by the New Approach: access to standardization processes and access to harmonized standards. It argues that although these issues are essentially European, their resolution depends on national institutions, which poses questions regarding the interplay between national and European accountability in standardization. Ultimately, it suggests possible solution to these challenges, placing them in the broader context of European standardization policy.

Keywords: New Approach – transparency – harmonized standards – copyright – AI Act

 Some parts of this paper benefited from author's earlier research on the project "Standards and Regulations", commisioned by the International Organization for Standardization (ISO). The author also would like to thank Richard Neerhof, Henk de Vries, and Anu Kostiainen for the very helpful discussions; and, the editors of this special issue, and the anonymous reviewer for their comments on the earlier drafts.

Recommended citation: Olia Kanevskaia, From National to European - And Back Again: Fixing the Flaws of the New Approach, 17 (2026) JIPITEC 20 para 1.

A. Introduction

1 Regulatory responses to technological advancement are in high demand. In the European Union (EU), co-regulation is becoming an increasingly used tool to manage, and respond to, various challenges stemming from the development and use of emerging technologies.[2] A vivid example is the "New Approach" regulatory technique, that allows market actors to demonstrate compliance with EU legislation through private voluntary harmonized standards (HSs). Initially designed with product safety in mind, the New Approach is increasingly being used in regulating digital systems and spaces, i.e., in the Artificial Intelligence (AI) Act,[3] Data Act,[4]

1 Assistant Professor of Public Economic Law, Utrecht University. Researcher, Utrecht Center for Regulation and Enforcement in Europe (RENFORCE).

2 Michèle Finck, 'Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy' (2018) LSE Law, Society and Economy Working Papers 15/2017; Nikita Divissenko, *Regulating Innovation in the Digital Age: A Demand-Centered Toolbox for the Data-Driven Economy* (Hart Publishing 2025) 89–90.

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 certain legislative acts [2024] OJ L 12.7.2024 ('AI Act').

4 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU)

and Cyber Resilience Act.[5] Furthermore, HSs are deemed essential for the EU strategic and critical sectors, such as security, medical devices, and education,[6] while they also promote the EU global competitiveness and ensure stability of the Single Market.[7]

2 Despite its notable success, the New Approach has also created a quandary for the European legislator. As HSs gradually enter the realm of public law, a substantial part of the regulatory authority is wielded by private standards development institutions, arguably without proper delegation of the rulemaking power. The legitimacy and constitutional issues trigged by this regulatory metamorphosis have been discussed at length in the scholarly literature.[8] Some of these challenges were reflected in a complaint filed by an NGO in September 2025 with the European Ombudsman, contesting the European Commission's role in ensuring transparency, inclusiveness, and accountability in standardisation processes leading to the adopting of HSs for the purpose of the AI Act.[9] There seems to be a general consensus among scholars and societal stakeholders that the New Approach is due for an overhaul.

3 In brief, the main challenges that the New Approach presents to the rule of law swirl around the issue of transparency and *access,* and in particular: 1) access to standardization processes through open and meaningful participation and 2) access to HSs that are copyright protected and, until recently, have been under the paywall.[10] These challenges are particularly pertinent to the EU digital legislation. Take, for instance, the AI Act, where abstract requirements for high-risk level AI systems are effectuated by HSs[11] and where, for the first time, such technical standards are going to be used in assessing compliance with fundamental rights.[12] Access to these standards is essential for compliance, while access to standards development processes is crucial for ensuring that standards are indeed responsive to, and compliant with, fundamental rights and ethical frameworks. But despite the recent case law developments as well as continuous calls for opening standardization processes,[13] the issue of access still presents a challenge.

4 In this paper, I argue that while restricted access to HSs and to their development processes is essentially a *European* problem, the institutional and policy design of the New Approach requires their solutions to be *national.* Quite paradoxically, while the ultimate responsibility for European standardization seems to rest on the European Standards Organizations (ESOs) and the Commission, it is the National Standards Organizations (NSOs) of the Member States that are the gatekeepers of standards and processes. Such a division of labor is mutually convenient, not least

2017/2394 and Directive (EU) 2020/1828 (Data Act) [2023] OJ L 22.12.2023.

5 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 [2024] OJ L 20.11.2024.

6 European Commission, 'An EU Strategy on Standardisation: Setting global standards in support of a resilient, green and digital EU single market' COM(2022) 31 final (hereinafter: 2022 Standardization Strategy).

7 See also Enrico Letta, 'Much More Than a Market: Empowering the Single Market to Deliver a Sustainable Future and Prosperity for All EU Citizens' (European Council, April 2024).

8 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; Linda Senden, 'The Constitutional Fit of European Standardization Put to the Test' (2017) 44 Legal Issues of Economic Integration 337; Megi Medzmariashvili, 'Delegation of Rulemaking Power to European Standards Organizations: Reconsidered' (2017) 44 Legal Issues of Economic Integration 353; Megi Medzmariashvili, 'Delegation of Rulemaking Power to European Standards Organizations: Reconsidered' (2017) 44 Legal Issues of Economic Integration 353, 353–66; Christian Joerges et al, 'The Law's Problems with the Involvement of Non-Governmental Actors in Europe's Legislative Processes: The Case of Standardisation under the "New Approach"' (1999) EUI Working Paper LAW No 99/9.

9 European Ombudsman, 'Complaint against the European Commission Concerning Transparency, Inclusiveness and Accountability in the Adoption of Harmonised Standards Related to Artificial Intelligence', Case 1974/2025/MIK (opened 26 September 2025).

10 Zachariah Davies and Arnaud Van Waeyenberge, 'Better Regulation by Standards? Harmonized Technical Standards, Transparency and the Rule of Law' (2025) 62 Common Market Law Review 147, 169.

11 See AI Act, 40 and recital 121.

12 For further critique on using the New Approach in the AI Act as a tool to uphold fundamental rights, see Nathalie Smuha and Karen Yeung, 'The European Union's AI Act: Beyond Motherhood and Apple Pie?' in: Nathalie Smuha (ed) *The Cambridge Handbook of the Law, Ethics and Policy of Artificial Intelligence* (Cambridge University Press: 2025) 228; Mélanie Gornet and Winston Maxwell, 'The European approach to regulating AI through technical standards' (2024) 13 Internet Policy Review 3; Marta Cantero Gamito, 'Artificial Intelligence co-regulation? The role of standards in the EU AI Act' (2024) 32 International Journal of Law and Information Technology.

13 ANEC and BEUC, 'For a "Standardisation Governance Act": ANEC and BEUC Recommendations to Adapt Regulation (EU) 1025/2012' (BEUC, 23 January 2024) <https://www.beuc.eu/sites/default/files/publications/BEUC-X-2024-001_For_a_standardisation_governance_act.pdf> accessed 6 June 2025.

because it allows ping-ponging responsibilities for providing access, as well as to forum-shop for the sources of legitimacy; but it ultimately creates an accountability gap and causes corrosion of European standardization policy.

5 My argument proceeds as follows. Upon explaining the link between European and national standardization (Section B), I will tackle the two transparency issues – access to ESOs' processes (Section C) and to HSs (Section D). I focus on the European Committee for Standardization (CEN) and European Committee for Electrotechnical Standardization (CENELEC), the two ESOs that share governance and operational frameworks and which are mandated by the Commission to develop HSs in support of the AI Act,[14] and I illustrate the national regulatory and policy landscape using the example of the Netherlands. Next, I will discuss the growing accountability gap that emerges from the current institutional set-up (Section E), and propose legal and policy solutions for "fixing" the access problems (Section F), before concluding my argument with a broader outlook on European standardization policy (Section G).

B. The Interplay Between European and National Standardization

6 In the EU, HSs ensure market integration and eliminate trade barriers between the Member States, which makes them the ultimate instruments of European harmonization. But reliance on standards in rulemaking practices is not merely an EU-wide phenomenon: standardization has a strong international dimension through the Technical Barriers to Trade (TBT) Agreement of the World Trade Organization (WTO),[15] and an equally important national dimension that can be traced back to the XIXth century and the industrial revolution.[16] While the New Approach has inherited traditions and practices from the national standardization systems of its Member States, current policy and academic discourses focus on the European, rather than national standardization actors, institutions and processes. This is not surprising: after all, the growing Europeanisation, the necessary national uptake of international and European standards,[17] and the obligation for NSOs to withdraw any standards that may conflict with HSs (the so-called "stand-still" requirement)[18] leave one to wonder whether national standardization is still relevant. Yet, as will be demonstrated in this section, the national legislation, policy, and NSOs play a crucial role in enabling European standardization.

I. Standardization at the EU Level

7 The history of the New Approach has been accounted for on multiple occasions.[19] As such, the New Approach, and later the New Legislative Framework,[20] was a response to the inefficient and labored process where harmonization requirements were highly detailed, top down, and binding, and developed through a legislative processes that required unanimity from the Council.[21] This mandatory reference was replaced in 1985 with the regulatory technique through which the European legislator established broadly defined health and safety requirements in its Directives, while technical standards concretizing these requirements were developed, upon the request of the Commission,

14 European Commission, 'Commission Implementing Decision of 22 May 2023 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' (Implementing Decision) C (2023) 3215 final.

15 Agreement on Technical Barriers to Trade (adopted 15 April 1994, entered into force 1 January 1995) 1868 UNTS 120, art 2.4. The link between international, European, and national standards falls outside the scope of this paper.

16 See Craig N Murphy and JoAnne Yates, *Engineering Rules: Global Standard Setting since 1880* (Johns Hopkins University Press: 2019) 19.

17 According to the recent data, an average of 86% of active HSs of CEN and CENELEC are transposed into national standards in all EU Member States. European Commission, Commission Staff Working Document, 'Evaluation of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation' SWD(2025) 171 final, 35.

18 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 [2012] OJ L316/12, 3(6) and recital 14.

19 See, for instance, some fundamental works of Harm Schepel, *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets* (Hart Publishing 2005); Joerges et al, above n 8; Jacques Pelkmans, 'The New Approach to Technical Harmonization and Standardization' (1986) 25 Journal of Common Market Studies 249.

20 The New Legislative Framework was adopted in 2008, updating the New Approach with regulatory instruments for strengthening the Internal Market, clarifying the functions of the CE marking, conformity assessment processes and market surveillance.

21 Council Resolution of 7 May 1985 on a New Approach to Technical Harmonisation and Standards [1985] OJ C 136/1.

by three ESOs: CEN, CENELEC, and the European Telecommunication Standards Institute (ETSI). Compliance with these HSs granted presumption of conformity with the European legislation.[22] ESOs operated according to their own governance rules and processes and consisted of technical experts that were seconded by the industry through national channels, i.e. NSOs.[23]

8 Were HSs meant to have legal effects already at that point? Presumably not. The fact that standards are "voluntary" has been underlined in many Commission's documents and communications, supported by the reasoning that, at least on paper, alternative means of compliance with the regulatory requirements were available.[24] Furthermore, and importantly, the New Approach was not an intentional delegation of the regulatory power, but rather drew a clear distinction between binding legislation, on the one hand, and voluntary standards that would ease compliance with that legislation, on the other.[25] This separation between standardization and rulemaking likely explains why free access to HSs and broader stakeholder involvement were not initially seen as points of concern under the New Approach.

9 The voluntarism of HSs undoubtedly contributed to the wider success of the New Approach, legitimizing this regulatory technique through availability of alternatives for demonstrating compliance with legislation. That said, these alternatives were either too burdensome or simply non-existent,[26] leaving the industry no other choice than conforming to the HSs. One may even suggest that the "voluntary" nature of standards may have served as a disguise for an unconstitutional delegation of authority.[27] The Commission may have as well been aware of the potential issues that such "delegation in disguise" have created, having an established practice of using experts to verify whether standards created by ESOs are indeed compliant with the legislative requirements.[28]

10 As the distinction between standards and law continued to blur, the European Court of Justice (CJEU) gradually pulled HSs into the public domain, conforming the legal effects of such standards on multiple occasions[29] and re-opening the constitutional questions on delegation of the rulemaking power to private actors.[30] For instance, scholars questioned the constitutional fit of EU standardisation within the EU legal order particularly in light of the limited Treaty safeguards governing the Commission's own powers,[31] and raised concerns about potential *abus de pouvoir* and the risk of undermining both the inter-institutional balance and the principle of conferral.[32] Further issues relate to the constitutional validity of delegating regulatory powers to ESOs, including possible non-compliance with the *Meroni* doctrine[33] due to insufficient supervision of the standard-setting process, limited judicial review, and the absence of accountability mechanisms for ESOs comparable to those applicable to EU institutions and agencies.[34]

11 These debates should be seen within the broader development of EU law being increasingly shaped not only by administrative bodies but also by standardisation organisations that enjoy considerable discretion in concretising and supplementing vague legislative requirements.[35] From this perspective, such potentially unconstitutional delegation of regulatory power to ESOs is particularly problematic

22 Commission of the European Communities, 'Completing the Internal Market: White Paper from the Commission to the European Council (Milan, 28–29 June 1985)' (White Paper) COM(85) 310 final, para 68.

23 See also 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, 149.

24 See the Commission's White Paper, above n 22.

25 See, for a similar argument, Joerges et al, above n 8, 5, arguing that the "world of thought lying behind 'delegation' both represents a distorted perception of constitutional problems along neat public/private and Community/Member State dichotomies and prescribes a misconceived solution to these problems."

26 Case C-588/21 P *Public.Resource.Org, Inc and Right to Know CLG v European Commission*EU:C:2023:509, Opinion of AG Medina, point 48.

27 See Joerges et al, above n 8.

28 Initially performed by the "New Approach Consultants" (NAC), and at present, by the Harmonized Assessment System (HAS) consultants.

29 See the landmark cases as Case C-613/14 *James Elliott Construction Ltd v Irish Asphalt Ltd* EU:C:2016:821; Case T-474/15 *Global Garden Products Italy SpA v European Commission* EU:T:2017:36; Case C-630/16 *Anstar Oy* EU:C:2017:971; Case C-588/21 P *Public.Resource.Org Inc v European Commission* EU:C:2024:201.

30 See the analyses of constitutional issues by Senden and by Medzmariashvili, above n 8.

31 Senden, above n 8, 338

32 Ibid, 343.

33 Case C-9/56 *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community* [1958] ECLI:EU:C:1958:7. Later in ESMA, Case C-270/12 *United Kingdom v European Parliament and Council of the European Union* [2014] ECLI:EU:C:2014:18, the Court justified the delegation of power to adopt the rules of general application to an EU agency based on technical expertise.

34 See also Vallejo on this point, Rodrigo Vallejo, 'The Private Administrative Law of Technical Standardization' (2022) 40 Yearbook of European Law 172, 175.

35 See in this regard Annalisa Volpato, *Delegation of Powers in the EU Legal System* (Routledge, 2022).

in the context of AI standards, given the significant fundamental rights implications and broader policy objectives at stake.[36] With the myth of voluntarism of HSs debanked by the CJEU, concerns surrounding delegation, although not the central focus of this paper, remain salient.

12 Another issue trigged by the increasing juridification of HSs was the financing of European standardization activities and, subsequently, the free access to the HSs that have become a "part of law".[37] This debate is not new: ESOs are dependent both on public (through the Commission) and private (through their members and, arguably, the sales of standards)[38] sources of financing. In this regard, the Commission suggested already in its 1990 Green paper that ESOs should make long-term financial commitments and change both the retribution of revenue from sales of standards and the membership fees for the industry; and even attempted to gradually cut back on lump-sum subsidies by switching to project-based financing.[39] This reiterates that the financing of European standardization activities is a policy baggage, entangled in a broader context of legitimacy and constitutionality.

II. Standardization at the National Level

13 Before globalisation instigated the need for cross-border harmonization and the creation of global and regional institutions, standards were largely produced by a homogeneous group of national industry actors, cooperating in loosely administrated processes shielded from political or market influence.[40] With the New Approach, these technical processes suddenly became central to the European integration; accordingly, standardization ceased being immune to institutionalization and Europeanization, as more structured standards bodies were required to operate at the EU level. This ricocheted to NSOs whose preliminary responsibilities as ESOs members became achieving the national level of consensus through consulting relevant stakeholders (public enquiry) and voting on acceptance of HSs.[41]

14 That said, standardization systems in Member States have significant differences, often embedded in national administrative laws and agreements made by NSOs with the relevant governmental bodies. The Netherlands provides an illustrative example: the Dutch NSO is the Royal Netherlands Standardization Institute (NEN). NEN develops national standards, including those that are based on, or implement, international and European standards. It is independent from the government but receives a task-oriented financing for its activities, including participation in ESOs, as per agreement with the Dutch Ministry of Economic Affairs.[42] Despite being an NSO and respecting the applicable CEN/CENELEC guides, NEN establishes its own procedures, participation rules and membership fees. While the current Dutch standardization system was largely inspired by the New Approach and presumption of conformity, it is still very much rooted in private sector traditions, where the industry initiated standards development[43] (unlike in the EU, where the initiative to develop HSs is the prerogative of the Commission). Similar to ESOs, NEN holds copyright over its standards, which – with the exception of standards that are made mandatory in national Dutch law, – are under the paywall.[44]

15 Standardization systems in EU Member States may also be contrasting. For instance, Germany, akin to the Netherlands, has a strong tradition of private standardization, whereas in France standards are part of the body of administrative law, and in Portugal, Spain and Greece, standardization used to be a public sector activity that then got privatized.[45] NSOs business models also vary in terms of funding mechanisms. In Finland, the NSO, SFS Finnish Standards, controls and coordinates almost all national standardization activities (with an exception

36 See Andrew Leyden, 'Standards and the EU AI Act: Legitimacy, State of Play, and Future Challenges' [2025] Information & Communications Technology Law 1, 16-17.

37 See also Olia Kanevskaia, 'Is it really all about the money? The future of European standardization after *PublicResourceOrg*' (2024) 16 European Journal of Risk Regulation 344.

38 But see Alexandru and Mateus Frazao Correia Magalhaes De Carvalho, 'Lawtify Premium: Public.Resource.Org (T-185/19), a Judicial Take on Standardisation and Public Access to Law' (2022) 15 Review of European Administrative Law (2022) 57, challenging the statement that sales of harmonized standards constitute a significant income for ESOs.

39 Commission of the European Communities, 'Commission Green Paper on the Development of European Standardization: Action for Faster Technological Integration in Europe' (Green Paper) COM (90) (1990) 456 final 66 – 73; see also Joerges and others (n 8) 18-19.

40 See van Gestel and Micklitz (n 23), 149.

41 CEN-CENELEC, Guide 4: General Guidelines for the Cooperation between CEN, CENELEC and ETSI and the European Commission and the European Free Trade Association (2003) 4.

42 See Ministerie van Economische Zaken en Klimaat, DG Economie en Digitalisering, 'Evaluatie van de taakgerichte financiering van NEN,' letter to the Parliment (19 March 2024) < https://open.overheid.nl/documenten/29b7f397-f6ed-4065-a98b-204452878deb/file> accessed 6 June 2025.

43 See also the opinion of AG in the Dutch Supreme Court case *Knooble*, Hoge Raad 11/01017 (30 March 2012) LJN: BW0393.

44 See Section D for further treatment of the issue.

45 See Joerges and others (n 8), 30, and the related references.

of electrotechnical and telecommunications sectors) including the selling of standards; however, national standards are developed in one of the 9 national standards writing bodies.[46] According to the SFS website, as of 2024, 97% of Finnish national standards were based on European or international standards, while sales of standards constituted about 80% of SFS's funding, and governmental financing amounted to 10% of SFS's funding.[47]

16 While these differences may fade for the European landscape, they remain important for national implementation of the HSs as well as for their access since, as we will see in Section D, HSs are sold exclusively through NSOs, often as "nationalized" standards translated into the national language. It is this interprlay between the European and national that sustains the EU standardisation but that ultimately gives rise to numerous challenges.

C. Access to Processes: Stakeholder Participation

17 Regardless of whether HSs arise from delegated powers,[48] participation in ESOs' is seen as one of the ex ante mechanism within the checks and balances of standardization processes,[49] which furthermore serves as a cornerstone of legitimacy and a complementary source of democratic input.[50] It is partly for this reason that broad stakeholder participation is one of the key priorities on the EU standardization agenda.[51]

18 The goal of broad and inclusive participation is typically directed at two types of actors. The first type can be generally categorized under an umbrella term "civil society": parties that are affected by HSs and have a keen interest in contributing to their development, but have been traditionally isolated from standardization processes, such as consumers, environmental organizations and non-for-profits. The extent to which these stakeholders are included in technical deliberations serves as a useful barometer for legitimacy of ESOs as institutions creating normative material,[52] addressing in part their democratic deficit and enabling consensus among the relevant stakeholders. At the same time, a truly meaningful inclusion of these stakeholders is often challenging due to the lack of funding and a steep learning curve of both the technical substance matters and institutional processes. Furthermore, consensus-building, which is an essential condition for standardization, often takes longer in a heterogenous group of actors,[53] while speed is crucial for the rapidly evolving technology markets.

19 The second type of under-represented stakeholders are Small and Medium Enterprises (SMEs) that amount to a large share of the European industry.[54] While SMEs participation in standardization processes is often essential to be able to access, and survive on, markets, their involvement is often not proportional to large companies, not least due to the lack of operational capacity, funding and technical expertise to tap into.[55] Increasing SME participation further prevents a capture by big market players, especially large non-European companies that dominate the global arena. Broadening the scope of participating actors thus serves two masters: increasing legitimacy of standardization processes and shielding them from unwanted foreign influence.

20 The aforementioned issues are particularly salient for AI standardization. AI systems and technologies integrate different components, which requires not only technical knowledge, but also expertise on fundamental rights and ethics to define and assess such concepts as "bias" and "fairness." In the EU, enabling the involvement of different stakeholders in AI regulation and governance goes beyond opening up ESOs, and includes the establishment of new institutions and processes.[56] However, such outwards-looking policy is a double-edge sword as

46 SFS Suomen Standardit ry, 'Standardointityö On Jaettu Usealle Organisaatiolle' (Standardization Work is Divided Among Several Organisations) (*SFS*) <https://sfs.fi/sfs-ry/meista/toimialayhteisot/> (machine-translated), accessed 8 January 2026.

47 Ibid.

48 See the analysis in Medzmariashvili (n 8).

49 Senden (n 8), 352.

50 See on this in relation to the delegated and implemented acts under Articles 290 and 291, Joana Mendes, 'Delegated and Implementing Rule Making: Proceduralisation and Constitutional Design' (2013) 19 European Law Journal 22.

51 See 2022 Standardization Strategy (n 6), 5.

52 See Annalisa Volpato and Mariolina Eliantonio, 'The participation of civil society in ETSI from the perspective of throughput legitimacy' (2024) 37(5) Innovation: The European Journal of Social Science Research, 1375.

53 See generally, Avinash Dixit, *Lawlessness and Economics: Alternative Modes of Governance* (Princeton University Press: 2007).

54 European Commission, 'Entrepreneurship and Small and Medium-sized Enterprises (SMEs)' (*European Commission*) < https://single-market-economy.ec.europa.eu/smes_en> accessed 6 June 2025.

55 See more generally on SMEs in standardization, Kirti Gupta, 'The Role of SMEs and Startups in Standards Development' (2017) < https://ssrn.com/abstract=3001513> accessed 6 June 2025.

56 The AI Act, for instance, establishes the European AI Board, that among other things, will consult the Commission when preparing standardization requests (Article 65), and the AI Office, which will help ensuring consistent implementation and enforcement of AI Act in the EU (Article 64).

the development of AI standards seems to take longer than expected, leaving the markets in a limbo.[57]

I. Stakeholder Participation at the EU Level

21 In general, there are two avenues through which stakeholders can get involved in the development of European HSs: 1) through Annex III of Regulation 1025/2010 as a European stakeholder organization receiving EU financing in accordance with Article 16 of this Regulation; or 2) through becoming an NSO member or participating in national standardization committees in any other way (e.g. as a stakeholder with voting rights limited to a particular committee or working group). The former seems to be preferred by the European legislator, as Article 5(1) of the Regulation 1025/2012 mandates wide participation and involvement of the relevant stakeholders in different stages of standardization. This obligation is clearly directed to the ESOs, which shall "*encourage and facilitate an appropriate representation and effective participation of all relevant stakeholders, including SMEs, consumer organisations and environmental and social stakeholders in their standardisation activities,*"[58] i.e., standards proposals, technical discussions, commenting, as well as in disseminating information about standards (but not standards themselves!). The wording of this provision suggests that not only should these stakeholders be able to attend the meetings of standardization committees ("appropriate representation") but also to meaningfully contribute to these meetings and, possibly, influence the outcomes ("effective participation").[59] This obligation is also echoed in the "Vademecum on European Standardization", which provides that ESOs have a reporting requirement to indicate how they have encouraged and facilitated, on the basis of Article 5, appropriate and effective participation of all relevant stakeholders, and furthermore provide the list of the categories of stakeholders participating in the development of harmonized standards.[60]

22 While the "European" avenue seemingly guarantees meaningful participation, it also has certain pitfalls. The beneficiaries of Annex III are limited to four types of organizations representing 1) SMEs; 2) consumers; 3) the environment and 4) social interests. To qualify for the funding of Article 16, these organizations must be non-governmental and not-for-profit, tailored to representing the respective stakeholders in European standardization and have a mandate to do so from at least two third of the Member States. Annex III thus does not enable direct participation, but rather a *collective* voice of a particular segment of stakeholders. Yet, SMEs' interest may vary per sector or even per Member State. Similarly, the overarching term "social interests" or "civil society" comprises divergent types of stakeholders whose positions may not always align, and who may experience participation barriers differently. As an example, while Regulation 1025/2012 encourages representation and participation of people with disabilities, Disabled Persons Organizations do not have voting powers in ESOs and are moreover faced with such challenges as a lack of adequate accommodation for participation in standardization meetings.[61] Even if some non-governmental organizations (NGOs) may be well equipped to represent the interests of these four types of stakeholders in European standardization processes, they are in an evident minority in ESOs technical committees, where the balance is typically tilted towards large technical companies. And while the recent reforms in the European standards bodies, notably ETSI, enhanced participatory rights of Annex III organizations, they are still far from being on an equal footing with technical actors.[62]

23 Furthermore, and notwithstanding the recent increase in EU funding for Annex III organizations and the Commission's subsidy to SMEs' representatives,[63] participation in ESOs remains costly for the both types of stakeholders, who moreover view the processes as too complex and time-consuming.[64] On

57 As such, CEN/CENELEC did not meet the initial deadline to adopt HSs for high-risk AI systems. While initially, the HS was supposed to build on the existing ISO/IEC 42001 standard on AI Management System, the discussions at the EU level revealed the incompatibility of this standard with the requirements of the Commission, leading to a longer standardization process. Such an assessment requires specialized knowledge and expertise to take part in the deliberations, while the market players would typically prefer efficient and fast standards development.

58 Regulation 1025/2012, 5(1).

59 See, in parallel, the concept of "meaningful" participation in WTO, 'Decision of the Committee on Technical Barriers to Trade on Principles for the Development of International Standards, Guides and Recommendations with Relation to Articles 2, 5 and Annex 3 of the Agreement' (1 November 2000) WTO Doc G/TBT/9 TBT, Annex 4, para C (7).

60 European Commission, 'Commission Staff Working Document: Vademecum on European Standardisation in Support of Union Legislation and Policies – Part III: Guidelines for the Execution of Standardisation Requests' (Staff Working Document) SWD(2015) 205 final, 2.6. Note that Vademecum merely serves as a guiding document in a form of soft law and does not impose any legal obligations.

61 'Evaluation of Regulation (EU) No 1025/2012' (n 17), 33-34.

62 For a "Standardisation Governance Act," (n 13); Volpato and Eliantonio(n 53).

63 'Evaluation of Regulation (EU) No 1025/2012' (n 17), 21-23.

64 Evaluation of Regulation (EU) No 1025/2012'(n 17), 33; see also High-Level Forum on European Standardisation, Workstream 3: NSBs Peer-Review (including SMEs and Civil

top of that, the scope of ESOs work has also expanded through the years, covering additional sectors and technologies, and thus requiring even more specialized knowledge and skills from stakeholders in ESOs' technical bodies.

II. Stakeholder Participation at the National Level

24 NSOs would typically agree on a national position among their stakeholders and then send (a) representative(s) to bring this position to ESOs, for instance through contributing to the discussions or voting on a standard's approval. This brings certain advantages: in ETSI, for instance, participation through NSOs allows direct voting power on the adoption of harmonized standards, while the votes of Annex III organizations are not counted in the new Approval Process.[65] What's more, NSOs can participate and vote in the international standards bodies: this means that they can take part in the JTC21, a joint technical committee of CEN/CENELEC which is focused on European standardization in the field of AI.

25 From this vantage point, participation in European standardization through the "national" avenue seems more attractive. For organizations that are not included in Annex III, this is the only option to be involved in standards development. In turn, SMEs enjoy enhanced participation guarantees at the national level, as Article 6(1)(b) of Regulation 1025/2012 explicitly requires NSOs to enable their participation in standardization activities even without NSO membership, while Article 6(1)(d) also requires to provide SMEs with free access to draft standards (which is currently the case only for 54% of NSOs).[66]

26 Yet, while NSOs largely follow the applicable CEN/CENELEC Guides, they establish their own participation rules, operational frameworks, and stakeholder strategies. NEN, for instance, distinguishes between the "regular" and "reduced" membership fees, with the latter applying equally to such categories as SMEs, NGOs and academia.[67] AFNOR, the French NSO, offers different membership packages tailored for different types of stakeholders, and even provides waivers to societal actors.[68] Such price differentiation is typically either enabled by agreements concluded between NSOs and national governments, i.e., ministries responsible for standardization policies, or by tailored subsidies that, again, are granted by the public sector. Financing models thus play a crucial role in providing meaningful opportunities for stakeholders' involvement in NSOs.

27 Furthermore, NSOs across the EU have different operational capacities. To illustrate, NSOs of larger Western Member States, like NEN, AFNOR, and German DIN, have a considerable standardization experience and are active players at the European and global levels; this is different for NSOs from smaller countries like Malta or Lithuania. Hence, an SME from the Netherlands would technically have more chances for their position to be heard in ESOs than a comparable SME in, for instance, Lithuania. This only exacerbates the already existent discrepancies between Member States. As a consequence, the involvement of underrepresented stakeholders in ESOs is fragmented and varies significantly across the NSOs. Recent numbers suggest that SMEs are represented in 31 out of 34 CEN/CENELEC members and 26 out of 39 ETSI members, while participation of societal stakeholders in NSOs varies between 47% and 77%.[69]

28 Most importantly, participation through the "national" route does not solve the issue of balance in stakeholder representation: after all, the majority of AI standards developers in JTC21 are corporate actors, with some large companies having more than one representative.[70] Rather, in the absence of effective opportunities under the "European route", the problem shifts to the national level. The effectiveness of stakeholder participation in European standardization thus hinges on the rules and processes of national standards bodies that are embedded in the legal systems and standardization policies of the Member States, and on the national financial instruments.

Society Inclusiveness) – Recommendations on National Inclusiveness (September 2024) < https://sbs-sme.eu/wp-content/uploads/2024/09/FINAL-Recommendations-HLF-WS-3-NSB-peer-review_v2.pdf> accessed 30 June 2025.

65 Mariolina Eliantonio and Annalisa Volpato, 'The European System of Harmonised Standards. Legal Opinion for EOCS' (2022) < https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4055292> accessed 6 June 2025, 32.

66 'Evaluation of Regulation (EU) No 1025/2012' (n 17), 22-23.

67 NEN, 'Normcommissielidmaatschap' (Standardization Committee Membership) (*NEN*) < https://www.nen.nl/normcommissielidmaatschap> (machine translated) accessed 6 June 2025.

68 AFNOR Group, 'Join AFNOR' (*AFNOR Group*, 2025) <https://www.afnor.org/en/about-us/join-the-association/#decouverte > accessed 6 June 2025.

69 'Evaluation of Regulation (EU) No 1025/2012' (n 17), 21-22.

70 Corporate Europe Observatory, 'Bias Baked in: How Big Tech Sets Its Own AI Standards' (*Corporate Europe Observatory*, 9 January 2025) < https://corporateeurope.org/en/2025/01/bias-baked > accessed 6 June 2025.

D. Access to Standards: Copyright and Distribution of Harmonized Standards

29 Public access to HSs has become a much-debated topic in the aftermath of the *PublicResourceOrg* judgement, where the CJEU held that HSs should be disclosed due to an overriding public interest.[71] These discussions are however not new at the national level, as courts of several Member States have previously ruled on the issue of access to national standards that have been equated to law.[72] The puzzle that the European and national courts are trying to solve boils down to the following: while standards bodies have legal ownership of the documents they create, and thus derive part of their income from their sales,[73] once their standards are used for regulatory purposes they acquire a "law-like" function and create binding obligations upon a wide range of actors. Hence, following democratic principles and the rule of law,[74] the texts of such standards should be available to those that are bound by obligations that these standards create. In other words, the law is not for sale.

30 The CJEU in *James Elliott* seemingly put an end to any doubts whether the presumption of conformity makes HSs truly binding by stating that HSs are a part of EU law owing to their legal effects.[75] The appeal decision in *PublicResourceOrg* confirmed it,[76] but left many issues unanswered, including the copyright protection of HSs and how and by whom should these standards be distributed to comply with the judgement. The following attempts to unpack some of these questions.

I. Access to Harmonized Standards at the European Level

31 The fact that the ESOs can hold copyright over HSs is as such not disputed by the New Approach.[77] In fact, the European Commission has previously recognized the sales of HSs as a legitimate mechanism of financing ESOs activities;[78] this recognition however came in times when standards' voluntary nature has not been questioned. CEN and CENELEC's exclusive copyrights over their standards are codified in Article 3 of CEN/CENELEC Guide 10.[79] The exclusive licenses for "publishing, reproducing and distributing" of HSs are however held by their NSO members, who are moreover responsible for making HSs, or their

71 *Public.Resource.Org,* para 85.

72 One of the very few systematic comparative studies on national case law, even though currently dated, was perfomed by Schepel and Falke. Their findings illustrate the divergent approaches and reasonings behind the national courts' decisions: in France, for instance, AFNOR holds a "monopoly" of standard distribution due to its public mission to develop and publish standards, but can nevertheless hold copyright under the French law, while in Austria, Greece, Belgium and Italy, the national courts ruled against the copyright retention. Harm Schepel and Josef Falke, *Legal Aspects of Standardisation in the Member States of the EC and EFTA,* Volume 1: Comparative Report (European Commission 2000) 168. Van Gestel and Micklitz, above n 23, followed later with the analysis of German and Dutch case law on the matter, noting the different conclusions of the courts. The German *Bundesgerichsthof* decision that DIN looses its copyright over private standards that are referenced in law, since their content is attributable to governmental officials who accepted and incorporated the standard, is particularly curious. Had this reasoning is applied to HSs, where the Commission plays a major role in approving, ESOs copyright over HSs may be seriously questioned. However, while public access justifies the exclusion of copyright in Germany, this does not seem to be the case in the EU where, as seen with ETSI, copyright does not preclude free availability.

73 The exact numbers remain unclear, although according to the figures reported by CEN, a loss of revenue from HSs sales would result in a significant deficit. See Davies and Van Wayenberge, above n 10, 169, citing CEN Annual Report 2021 and 2022, both available at < https://www.cencenelec.eu/news-and-events/news/?News%20types[]=3690>. Most recent numbers sugges that for all three ESOs, harmonised standards account for 11% of all standardisation deliverables produced between 2013 and 2024, 'Evaluation of Regulation (EU) No 1025/2012' above n 17, 11. See also annual report 2024 https://www.cencenelec.eu/news-events/news/?News%20types%5b%5d=3690.

74 See the discussion in Volpato, above n 8.

75 *James Elliott,* para 40.

76 *Public.Resource.Org,* para 70.

77 Although it was challenged by some academic commentators, see Alexandru Soroiu, 'The CJEU Dismantles EU Standardisation in C-588/21 P (Public.Resource.Org)" (Verfassungsblog, 19 March 2024) < verfassungsblog.de/eu-harmonised-standards/> accessed 7 June 2025; Sunimal Mendis and Olia Kanevskaia, 'Harmonized technical standards under EU copyright: the Public.Resource.Org judgement' (IPKat, 22 July 2024) <https://ipkitten.blogspot.com/2024/07/harmonized-technical-standards-under-eu.html> [date accessed].

78 Harm Schepel and Josef Falke, Legal Aspects of Standardisation in the Member States of the EC and EFTA, Volume 1: Comparative Report (European Commission 2000) 168, note 10, citing M. Bangemann, in response to Written Question No. 822/91, MEP M. Welsh, (1992) OJ C 2/10.

79 CEN-CENELEC, *Guide 10: Policy on the Distribution, Sale and Copyright of CEN and CENELEC Content*, 5th edn (2024). Specific rules apply to 'Eurocodes', HSs supporting the construction sector; CEN-CENELEC, *Guide 28: Guidelines for the Public Access of Eurocodes and Their National Annexes and Harmonised European Standards under the Construction Products Regulation*, 1st edn (19 June 2014).

translations, available nationally.[80] The licensing terms are defined in the agreements between the ESOs and NSOs,[81] and prices are generally based on the number of pages per document. In this regard, while NSOs enjoy a considerable freedom to set their prices and sales conditions (e.g. discounts for standards bundles), revenues yielded from these sales are given to CEN/CENELEC as their legal owners.[82] This disconnect between rights holders and distributors is not uncommon in copyright law,[83] but in the context of the New Approach, it presents challenges to public availability of *European* standards that, apparently, should be manifested at the national level.

32 These challenges particularly concern NSOs since, without the revenue from standards' sales, they should find an alternative source of income to support their activities and/or to pay dues to CEN/CENELEC.[84] What's more, CEN/CENELEC Guide 10 provides NSOs that do not comply with the copyright and distribution policy risk being excluded from participation in standardization activities or even expelled from the ESOs membership.[85] At the same time, when a breach of ESOs' copyright through unauthorized reproduction or distribution of standards is suspected in the Member States territory, the responsibility to start an individual action lies with the Member State concerned.[86] In this regard, NSOs also have a "last resort mechanism" for the purpose of responding to requests for free access to the standards to the general public: in fact, CEN/CENELEC Guide 10 prescribes that its Members first should use all reasonable efforts to reject such requests, and only grant a sponsored conditional access in close consultation with CEN/CENELEC.[87] It should be noted that, while these provisions are clearly not in compliance with the *PublicResourceOrg,* the current version of the Guide at the moment of writing is the one of January 2024, and thus predates the CJEU decision; accordingly, significant updates of these provisions may be expected in the new versions of the guide.

33 Furthermore, akin to many national standards, HSs implement or are based on standards developed by other bodies, such as ISO and IEC.[88] Making HSs publicly available thus automatically triggers these bodies' copyright, possibly resulting in potential breach of contract and violation of intellectual property rights and affecting the ecosystem of international standardization.[89] Curiously, Guide 10 states that each participant or contributor, including, under specific terms ISO and IEC, that is involved in the development of European standards must grant the rights to their contribution to CEN/CENELEC, which then have the rights to exploit this content worldwide in any format and grant exploitation rights to NSOs and partner organizations.[90] This provision, however, seems to concern contribution of these bodies to HSs development processes and does not stretch to standards that are used as a basis for such HSs.

34 Yet and as confirmed in the recent *Stichting Rookpreventie II* judgement of the Court of Justice[91], ESOs copyrights over HSs, while seemingly undisputed, do not preclude standards availability: for instance, ETSI's standards can be accessed free of charge, and ETSI still retains copyright over them. Hence, whether ESOs will indeed suffer financial consequences as a result of their standards being made publicly available, as it was claimed by CEN/CENELEC in the General Court,[92] largely depends on their business model.

80 CEN-CENELEC, *Guide 1: Status of European Standards*, 1st edn (December 2001), 1; see also Guide 10.

81 CEN-CENELEC, *Internal Regulations, Part 1: Organization and Structure* (1 January 2025), clause 1.5

82 Guide 10, Annex A.

83 Think, for instance, of commercial publishing industry, where the author of the original work is a right holder, but the revenues from distribution largely go to the publishing house.

84 Van Gestel and Micklitz, above n 23, 147, note that previously, NSOs were not able to provide figures for sales of HSs and revenues from them.

85 Guide 10, 1; see also CENELEC, *The Statutes of CENELEC* (adopted 27 June 2024, entered into force 1 January 2025), 9.1.2.

86 Guide 10, 7 (e).

87 Guide 10, 9.

88 Davies and Van Wayenberge, above n 10, 154, note that based on the figures reported by CEN and CENELEC for the first quarter of 2024, approximately 44 percent of all HSs developed by these ESOs were identical to (circa 38 percent) or based on (circa 6 percent) standards published by the ISO or the IEC. More recent data from CEN and CENELEC 2024 Annual Report demonstrates that 62,1% of HSs (779 out of 1.355 HSs published in 2024) were identical to those of ISO and IEC, making the percentage of total standards developed by CEN and CENELEC and that are identical to ISO and IEC international standarrds about 49,6 % (11.129 out of 22.457). CEN and CENELEC, *Annual Report 2024,* < https://ar2024.cencenelec.eu/ > accessed 8 January 2026.

89 At the moment of writing, a case is pending before the EU General Court brought by IEC and ISO against the European Commission, alleging a breach of copyright resulting from the distribution of harmonised standards based on IEC and ISO materials. Case T-631/24 *International Electrotechnical Commission and ISO v Commission* OJ C/919.

90 Guide 10, 3.

91 Case C-155/24, Nederlandse Voedsel- en Warenautoriteit and Others v Stichting Rookpreventie Jeugd EU:C:2026:327 ("Stichting Rookpreventie II").

92 Case T-185/19 *Public.Resource.Org, Inc. and Right to Know CLG v European Commission* EU:T:2021:445, para 66.

35 In this regard, the question that *should* be asked is who is responsible for providing access to these standards.[93] Pursuant to the Vademecum on European standardization, both ESOs and NSOs are expected to seek suitable ways of to make publicly available information that indicates legal requirements covered by a HS as well as information on significant changes to harmonized standards, especially when it comes to providing these to SMEs.[94] This transparency requirement is not an obligation to make the *content* of these standards publicly available, although it is unclear how information on standards' modifications can be useful to stakeholders who do not have access to the text of these standards. It is also in conflict with the earlier Communication of the European Commission on Intellectual Property Rights and Standardization, which provides that standards bodies may lose their status as an ESO if they fail to ensure non-discriminatory access to standards,[95] as well as with Article 6 of Regulation 1025/2012, which lays on the NSOs the obligation to ensure SMEs' access to HSs and, given the lack of any enforcement mechanisms at the EU level, leaves NSOs with a broad discretion to decide how this access should be facilitated. That said, parts of the legal framework that provides these obligations are, again, outdated, since the current version of Vademecum predates the landmark rulings on CJEU. Hence, as it is the case with CEN/CENELEC Guide 10, an update can be expected that will clarify transparency obligations of ESOs and NSOs .

36 The aforementioned Commission's IPR communication introduces yet another important actor in this equation, namely the European Commission itself, which should ensure that all interested parties have access to standards on "fair, reasonable and non-discriminatory basis"[96] when these standards are referred in legislation as mandatory requirements or "as one which confers a particular status under Community law" (possibly meaning the presumption of conformity). What's more, if the Commission believes that a standard is not being made available on these terms, it must withhold or withdraw the standards' approval as a HSs. While this seemingly puts the Commission in the driving seat (which largely follows the line of reasoning of Advocate General Medina),[97] the Commission acting as a catalyst of access to HSs does not square with ESOs' exclusive ownership rights, and NSOs exclusive rights of distribution and reproduction.

II. Access to Standards at the National Level: The Netherlands

37 At the national level, some remarkable discussions on the legal force and accessibility of private standards referenced in law took place in Court rooms and legislative chambers in the Netherlands, making this a good case study for the purpose of this paper. As other EU Member States, the Netherlands has its own legal understanding of standards, rooted in its constituonal traditions and national legislation. Not all standards refenced or cited in the Dutch legislation are considered mandatory. The Dutch Building Decree[98] – a textbook case of the reliance on private standards in safety regulation –,[99] is an illustrative example. While the provisions of the Building Decree refer to a number of NEN standards and convey an impression that the use of these standards is mandatory, the "equivalence clause" of Article 2.5 stipulates that other means of compliance may be used to demonstrate compliance with the requirements of the decree: accordingly, standards in the Dutch building legislation merely raise a presumption of conformity but are not equal to law.

38 The non-mandatory nature of such standards has been confirmed in case law. In 2012, some years before *James Elliott*, the Dutch Supreme Court ruled in *Knooble* that the reference to NEN standards in the Building Decree indeed pulls these standards into the public domain due to their legal effects, but does not make them "laws", since these standards were not published following the procedure that published laws and NEN's function of standards developer is not based on the delegation of public authority.[100] Rather, the Court held that such standards are "outwards applicable general rules"

93 The CJEU in its recent decision Stichting Rookpreventie II ruled that it is irrelevant whether such acccess should be ensured by the EU or its Member States resources, but that it is the EU which has to bear the costs associated with access., see Stichting Rookpreventie II, para 40.

94 Vademecum, above n 61, 2.10.

95 Commission of the European Communities, 'Communication from the Commission: Intellectual Property Rights and Standardisation' COM(92) 445 final (Brussels, 27 October 1992), 6.3.2 and 6.3.3.

96 Fair, reasonable, and non-discriminatory terms (FRAND) refers to the obligation to provide access to property subject to exclusive rights, and is commonly used, for instance, in the licensing of standard-essential patents.

97 AG Opinion in *PublicResourceOrg*, above n 26, para 28.

98 Besluit bouwwerken leefomgeving (Stb 2021, 71), in force from 21 May 2025.

99 See, among others, Richard Neerhof, *Bindende werking van private normen en regels in het privaatrechtelijke bouwrecht* (IBR Publications 2023).

100 Gerechtshof 's-Gravenhage, 16 November 2010, ECLI:NL:GHSGR:2010:BO4175, case nos 200.029.693-01 and 200.031.136-01, 8-9 and 14; confirmed on appeal in Hoge Raad, 22 June 2012, ECLI:NL:HR:2012:BW0393, case no 11/01017 Reference. See also the discussion in van Gestel and Micklitz, above n 23.

that are established on the basis of private law agreements, and it is sufficient if they are available for commercial firms against a "reasonable fee" (without specifying what is reasonable) or can be viewed publicly without hindrance, for instance at the NEN library. [101] Hence, unlike claimed by the plaintiffs, it was not required for the text of these standards to be published in the Dutch State Gazette (*Staatscourant*) as laws and governmental regulations. In a parallel case adjudicated by the Administrative Division of the Council of State, the judges followed the similar reasoning and found that standards that do become binding as a consequence of their reference in the Building Decree, are "outwards generally binding rules", and thus should be announced in *Staatscourant.*[102]

39 In the aftermath of *Knooble,* the practice of referencing NEN standards in national laws and regulations have been brought to the attention of the Dutch Parliament.[103] Two important outcomes of this discussion, that also shaped the current Dutch policy on standardization, were the following: Firstly, standards referred to in national laws and regulations should in principle remain voluntary.[104] However, and secondly, once standards *do* become mandatory as a consequence of this reference, they should be made publicly available free of charge and published as law pursuant to Article 89(4) of the Dutch Constitution. In this regard, the Dutch Drafting Instructions for Legislators name certain cases when the legislator may opt for mandatory compliance with the standard, i.e., when such mandatory obligations are required by EU law, Treaties and decisions of international organizations; or when the regulations at issue are directed towards the governmental institutions where the exclusive application of such standards is desirable or concern the enforcement of criminal norm (for instance in case of measuring methods).[105] In any case, such mandatory reference should be motivated and foreseen by information about where the standard can be found. The requirement of public availability thus only applies to standards that have acquired a public-law character through their citation, or reference to them, in the legislative or regulatory text.

40 Figure 1 schematically illustrates the requirements for standards availability in the Netherlands,

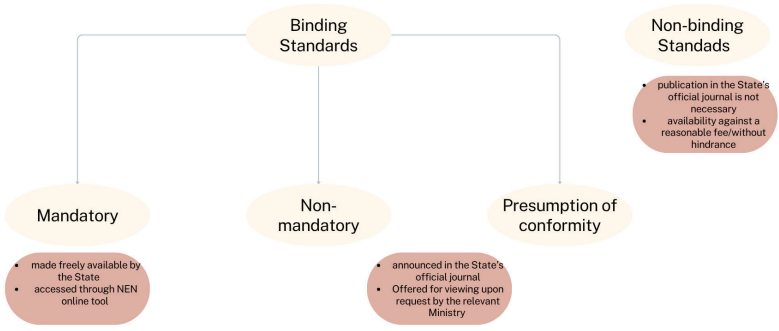

Figure 1: requirements for access to standards in the Netherlands

41 But even if these law-like standards are equated to law, NEN does not cease to hold copyright over them meaning that, at least in theory, offering these standards free of charge inevitably results in the loss of income and affects NEN's ability to finance its standardization activities. As a solution, the Ministry of Economic Affairs in the Netherlands "buys off" NEN's standards that have become mandatory through their reference in the text of law, hence compensating NEN for the (potential) loss of income.[106] In turn, NEN provides such mandatory national standards, and, in the aftermath of *PublicResourceOrg,* HSs free of charge through its online tool upon a free registration.[107]

42 That said, this agreement is only valid between the Ministry and NEN, and hence only applies to NEN homegrown standards. A similar arrangement will not work for HSs and international standards that have been made mandatory through their incorporation and hence, according to Dutch law, should be made publicly available; what's more, placing these standards into public domain will result in the breach of the copyright policy of standards bodies that issued these standards in the first place (although the situation is different for ESOs after the *PublicResourceOrg* ruling).[108] Hence, the Drafting Instructions for Legislators provides that if a mandatory reference is made to an *international*

101 Gerechtshof 's-Gravenhage, 7.

102 Raad van State, 2 February 2011, ECLI:NL:RVS:2011:BP2750, case no 201002804/1/H1, 2.4.5 and 2.4.6.

103 Minister van Economische Zaken, Landbouw en Innovatie, *Brief aan de Voorzitter van de Tweede Kamer der Staten-Generaal: De kenniseconomie in zicht*, Kamerstukken II, 27 406, nr 193 (30 June 2011).

104 Rijksoverheid, Aanwijzingen voor de regelgeving (Stcrt. 1992, 230), 3.48.

105 Ibid.

106 The invoice is provided on the basis of the downloads through online tool, NEN connect.

107 While functional, the tool still has certain limitations. See the case study conducted by (2025) <Linda Zhou, Bas Tissing and Freek van den Oetelaar, 'Project Report: Copyright and Standards' (ILP Lab 2025).<https://ilplab.nl/projects/report-on-opening-technical-standards-and-copyright/> accessed 8 January 2026.

108 See above n 89 and accompanied text.

standard, the price of this standard should not be "unreasonably high"[109] – without, again, defining what "unreasonably high" is and whether, in case the costs of access prove too burdensome for certain stakeholders, they will be mitigated by the State.

43 There is a striking difference between the treatment of the legal effects and presumption of conformity stemming from private standards by the Dutch and European Courts. While in the EU, the fact that standards have legal effects seems to place them into the domain of lawmaking, and thus require these standards to be publicly accessibly based on the rule of law principles and transparency requirements, the Dutch Supreme and Administrative Courts appear not to consider the legal effect of standards sufficient to equate them with the law, and base their decisions on the *source* of the rulemaking authority and their delegated powers. From this vantage point, the conclusion of the Dutch Courts that such standards retain their copyright and should not be made publicly accessible is not astonishing, although the reliance on the vague terms as "reasonable fees" or "reasonable availability" for access to these standards ideally requires further refinement. It is curious however, whether the reasoning of the CJEU would have led it to arrive at the different conclusion than the Dutch Court regarding the copyright protection of HSs. Either way, the question remains whether the Dutch case law, and thus also Dutch standardization policy, will still hold in the aftermath of *PublicResourceOrg* and *Stichting II.*

E. The Expanding Accountability Gap of European Standardization

44 A closer look at the New Approach reveals that it is full of paradoxes that are not easy to resolve. Free access to HSs is desirable yet will likely obstruct the proper functioning of the European standardization system. ESOs' and NSOs' funding depends on the sales of HSs through NSOs yet little research has been done to verify whether and to what extent this is actually the case, as consolidated figures of overall annual EU expenses for standardisation are also unavailable.[110] Most importantly, while providing access to standards and standardization processes is a European requirement, the institutional settings and lack of enforcement of Regulation 1025/2012 at the EU level leaves the *onus* of this obligation on NSOs and Member States. There is nothing "European" about access to European standardization.

45 Even bigger disconnect lies in the shared obligations of European and national bodies, where the Commission requests and approves HSs, ESOs owns HSs and are responsible for the their content, and NSOs distribute HSs while operating within the framework set by national governments. The accountability of governmental bodies appears to be triggered only when standards acquire legal effect through a governmental action, either by the Commission's approval and publication of a standards' reference in the Official Journal of the EU (OJEU) or, in case of Member States, by a regulators' decision to cite a standard in a regulatory document and, at least in the Netherlands, couple this citation with an obligation of compliance.[111]

46 Being the sole license holders for selling HSs in their respective Member States, NSOs find themselves in a bind, bearing the ultimately responsibility of correctly implementing the *European* standardization policy through *national* measures that are often divergence, if not contradictory, to the European requirements.

47 It should not be forgotten that Member States can exercise influence over the HSs even before those are formally adopted into the European legislation and cited in the OJEU, for instance through Articles 10[112] and 11 (formal objection) of Regulation 1025/2012. Similarly, the Commission's power to direct the private ordering of European standardization seems to have grown in prominence over the years: while in past, reforms proposed by the Commission in its Green paper were fiercely opposed by the industry and ultimately abandoned, institutional amendments introduced in the 2022 Standardization Strategy and Regulation 2022/2480 have been, even though reluctantly, implemented by ESOs.[113] But when it comes to providing access as a part of wider transparency obligations, both the Commission and Member States appear hesitant to use the tools available in their regulatory toolbox.

48 On top of that, this already fragile system of interplay between private and public, national and European, hinges on stretched competences conferred upon bodies whose status under EU law remains uncertain. This is an important point from the constitutional perspective, as the legitimization of the New Approach in its current form appears to rest, on

109 Aanwijzingen voor de regelgeving, 3.48.

110 'Evaluation of Regulation (EU) No 1025/2012' above n 17, 43.

111 This entanglement into natinal legal systems may be not to the liking of constitutional pluralists. See the discussion in Vallejo, above n 34, at 184 and 210, engaging with Schepel's seemingly pluralistic take on the legal status of HSs.

112 According to Senden, the rationale behind Article 10 is to mitigate insufficient public and democratic control, and prevent the risks of capture by business interests, Senden, above n 8, 343.

113 See Panagiotis Delimatsis and Zuno Verghese, '"To Antipolis, my sisters!": ETSI as a forum of contestation, collaboration and orchestration' (2024) 37 Innovation: The European Journal of Social Science Research 1305.

the one hand, on voluntarism, and on the other, on checks and balances ensured through administrative and judicial control. In a rather paradoxical manner, the former seems to have diminished as the latter has expanded, revealing the flaws in the system's design.

49 It follows thus that the current institutional and legal landscapes of the New Approach points towards NSOs as the ultimate actors capable of resolving this accountability gap. But such solution comes with criticism and limitations. Firstly, NSOs operate within the national frameworks and in principle can only create rules applicable to national standards. Even if disentangling national standards from European and international ones presents a challenge, overstepping NSOs' competences may trigger legal actions against them or even a Member State. Secondly, and as demonstrated in Section D, Member States' approaches to access to standards documents and processes are intrenched in national laws and differ in terms of funding and resources available nationally to support and promote standardization activities. This inevitably prevents a common approach across all 27 Member States, potentially rising constitutional issues at the national level and risking divergent interpretation and implementation of European standardization policy.

50 In particular, the differences in prices and sales conditions for HSs across NSO lead to inequalities among the Member States when it comes to transparency and access to normative material that, per CJEU case law, has become "a part of EU law." Firstly, it enables forum-shopping among standards users, some of which may be inclined to acquire technical documents by cost-friendly NSO (a practice that anecdotally does not occur too often due to the "gentlemen' s agreements" among NSOs and domestic industry players.) Secondly, these differences preclude correct implementation of Article 6(1) of the Regulation 1025/2012, as the issue of SMEs' access to standards becomes a matter of agreements between NSOs and national governments, where the latter may decide to compensate an NSO for the loss of income that occurred due to the privileged prices for certain stakeholders. This makes national governments intermediaries that fix the lacunae in the agreements between ESOs and NSOs. Such practice of State compensation is common in some European countries, like France and Spain, but is not applied in others, like the Netherlands which, again, adds to discrepancies between national implementation of European rules. Member States thus enjoy a wide discretion when designing their standardization policies and applying their administrative laws to both national and European or international standards. These national regulations, together with the terms of agreements between NSOs and ESOs or national governments, shape the NSOs policies and practices on access to standards documents and standards processes.

51 From a different viewpoint, leaving the matters in hands of NSOs also comes with certain benefits. At the outset of the EU project, national governments have already been asked once to give up some of their regulatory powers in favour of the European Commission; with the New Approach, these powers are once again being wielded, this time to private actors, arguably without a proper act of delegation and with even less control and oversight. The fact that the role of the NSOs has been gradually increasing throughout the years, first moving from merely advising to approving the HSs,[114] and recently gaining the exclusive powers to vote on HSs,[115] are some steps in the direction of inviting more national power and constitutional checks and balances to the New Approach.

F. Fixing, Not Fixating

52 Discussions on access to standards and standardization processes have animated legal scholarship long before *PublicResourceOrg* and, more recently, *Stichting II*;[116] with the Court's rulings, however, the need for pragmatic solutions has become even more evident. One thing is clear: the system of the New Approach, however deficient, has proven to work well for the European integration. The alternatives are gloomy: in the absence of standards, it is the EU and its Member States that will have to develop detailed technical specifications – a task for which they inherently lack time and resources. At the same time, letting standards slip into the domain of private ordering without any public oversight risks fragmenting markets and defeating technical harmonization. Given the institutional and regulatory complexities, how should the New Approach be revived to remain functional yet respect the rule of law?

53 The only solution that has been adopted so far, namely a read-only online portal developed by CEN/CENELEC to be used by NSOs, once again illustrated the tendency of shifting European challenges to the national level. The functionality of this tool allows anyone to consult the text of HSs but precludes from making any copies or screenshots of the document. This tool, I argue, is a lip service to the

114 Joerges and others, above n 8, 48.

115 See Regulation 2022/2480.

116 See, for instance, Bjorn Lundqvist, 'European Harmonized Standards as Part of EU Law: The Implications of the *James Elliott* Case for Copyright Protection and, Possibly, for EU Competition Law' (2017) 44 Legal Issues of Economic Integration 421.

PublicResourceOrg judgement: it only solves the problem of access, and not distribution, missing the bigger picture of free availability of legal texts and the rule of law. Furthermore, and due to the lack of feasible European alternatives, NSOs may consider revisiting their financing model, focusing for instance on producing and selling value-added versions or documents essential for standards' implementation. While understandable from the business viewpoint, such practice risks rendering HSs incomplete or even futile without those additional documents and thus negates the very core of the argument that legal obligations should be known to the public. It seems that the current cure for European standardization is worse than its ailment.

54 Though not intended as a panacea for all flaws of the New Approach, this Article proposes several remedies for fixing the issues of access.

55 Firstly, there is a need to update the current legal framework and policy documents in which European standardization is grounded. Given the case law developments of the past decade, it is striking that the Vademecum has not been updated since 2015, and that Regulation 1025/2012 refers to standards as "voluntary".[117] Article 5 of the Regulation should also be clarified as to the degree of responsibilities that the ESOs and NSOs bear for ensuring a wide stakeholder participation, as should be the role and responsibilities of the European Commission. Furthermore, the Commission should formulate a clear position regarding the consequences of *PublicResourceOrg* decision for ESOs' copyrights and accessibility of standards, which would help clarify the obligations of different actors and institutions of the European standardization ecosystem and fill in the gaps left by the CJEU.[118] Of course, legal and policy changes are notoriously slow to implement, and by the time amendments have been adopted, many acutely needed HSs, such as those in the field of AI, will be already developed and on the market. Nonetheless, greater coherence in European standardization policy could strengthen both the policy framework and the European project, by articulating a clear common position without altering Member States' laws.

56 Secondly, this Article suggests that the inevitable reliance of the EU standardization on agreements between ESOs and NSOs on the one hand, and NSOs and States on the other, artificially fragments the system of standardization. Rather, or additionally, this type of agreements should be concluded between the Commission and Member States. The existing agreements between ESOs and NSOs should also specify conditions for privileged access to HSs standards and to ESOs' processes, strengthened by the commitment of funding from either Member States or the Commission. While ESOs and NSOs may initially be expected to resist this intervention or view it as encroaching on their contractual relationships, they may also consider it a welcome a shift of access and allocation of responsibilities discussions to those with the actual power to address these challenges.

57 Thirdly, HSs should be made available directly through ESOs, rather than NSOs.[119] Currently, once HSs or international standards are referenced in legislation, they become a subject of national administrative law. The issues as accessibility, distribution and reproduction of such standards then become tied to the question whether they acquire a legal force and result in a binding obligation. In this situation, national legislation and judiciary decisions may clash with NSOs' contractual obligations to ESOs and other standards bodies in case they prescribe for their standards to be freely available.[120] While this may indeed put more burden on the ESOs, it also opens opportunities for their increased cooperation with NSOs on such issues as translation and distribution of standards document. Such cooperation could then level the playing field for the European industry and citizens by setting similar conditions for HSs accessibility. This is of course easier said than done, since national differences in administrative and copyright laws remain applicable to HSs that are cited in national regulations. For these reasons, the terms of this arrangement should, again, be prescribed in the agreements between ESOs and NSOs.

58 Finally, there are always options for Member States to streamlining their standardization policies, and for NSOs to make their processes more inclusive. In

117 In contrast, at the national level, landmark case law has led to more prominent legislative changes to access policies, or even amendment of national copyright laws and introduction of compulsory licensing, see discussion in van Gestel and Micklitz, above n 23. On top of that, the definition of HSs appears inconsistent with the terminology of the General Product Safety Regulation (GPSR), leading to incoherences for standards requesting processes, 'Evaluation of Regulation (EU) No 1025/2012' above n 17, 57. It should also be noted that at the moment of writing, the amendment process of Regulation 1025/2010 is still ongoing.

118 See, for a similar argument, Davies and Van Wayenberge, above n 10, 165.

119 This resonates with the advanced financing mechanisms and the increasing role of ESOs in sellings standards proposed in the 1990 Commission's Green Paper.

120 On top of that, interpretation of "public availability" seem to differ in national laws: for instance, in France "public availability" seems to include paywalls, while in the Netherlands, it also covers physical-only access at the NSO premises. Zhou et al, above n 106.

this regard, ESOs, but also the European Commission, can continue serving as facilitators, inviting NSOs and Member States to share their best practices and to learn from each other. In this context, stronger and more experienced NSOs can play a meaningful role in supporting less experienced ones through agreements, capacity-building, education, and exchanges. While changes to national laws are neither feasible nor desirable, such streamlining can nonetheless promote greater coherence across the system. This coherence is crucial especially in the rapidly developing field as AI, where the EU ambition is to become a global standard setter while also preserve its European values[121] requires Member States to speak with one voice.

59 Although each of these solutions entails costs, they offer greater durability and bring standardization closer to the rule of law, while preserving the balance between private expertise and public accountability.

G. Conclusion

60 The New Approach exemplifies a fundamental tension between private expertise and public accountability, in which traditional boundaries are deliberately blurred. Private expertise is indispensable, and one of the principal strengths of the New Approach has been its ability to preserve and mobilize such expertise—an attribute that remains essential for AI and standardization more broadly. At the same time, public accountability has become increasingly salient as standards, including AI standards, acquire greater public significance. Even if the New Approach was conceived not as a form of delegation but as a system of accountability, it is evident that the system is now failing.

61 In this light, access to HSs and standardization processes becomes particularly crucial. To comply with the legal requirements for high-risk AI systems and anticipate market developments, industry actors need HSs before the relevant provisions of the AI Act are fully enforceable. At the same time, the increased participation of Annex III organizations and SMEs in standards development, while necessary due to the specifics of AI as well as for the alignment of these standards with EU democratic values and interests, delays the speed with which HSs for AI are created. What's more, AI in itself is a moving target: the recent soar of Large Language Models (LLMs) and Generative AIs, and the consequent hasty changes to the draft AI Act in 2023, confirmed yet again how technology development outpaces regulatory efforts. Hence, if we are to regulate AI with the New Approach, we need to preserve its benefits, and to release what no longer serves us.

62 In this regard, the recent line of case law raises a lot of questions on the limits of private ordering of European standardization, the legal value of European standards and the role of ESOs as semi-regulators. These questions touch upon some very fundamental constitutional issues, such as competences to regulate and shared accountability for the legal material produced outside public bodies. While these questions are not without merit, it should be recalled that the European standardization has never been about the delegation of powers in the first place, but rather about bring private powers into the public sphere.[122] In this context, HSs have been meant as opposites to the law: a non-binding product of the industry, for the industry, aiming to bring agility to public policy, but not to replace it. By a curious chain of contradictions, it is the very voluntary nature of HSs that led them to have legal effects and cause the current impasses, where the challenges of integrating private expertise into law-making became a discussion on the rule of law and, eventually, should be solved through financing.

63 But while rooted in technical complexities and layers of regulation, this discussion also runs deeper, illustrating a common EU problem of safeguarding "European" through "national". In this regard, as the New Approach generated path dependencies that in a way limit the flexibilities of future regulatory reforms, it is also likely to pass on the issues of transparency into different domains, adding to the urgency of addressing these issues now. Fixing the system is not just about making HS publicly available, but revisiting deep-rooted problems stemming from past intentions.

64 It will most likely take a long time and a chain of litigation processes and policy changes before this impasse is resolved. In the meantime, it is worth remembering a common aim that underlies the effort to find the solution: a strong Internal Market in the EU that is based on the rule of law.

121 See AI Act, 40 (3) and recitals 1,2,6; Mario Draghi, *The Future of European Competitiveness: Part A – A Competitiveness Strategy for Europe* (Publications Office of the European Union 2024) 5 < https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en> 5, accessed 7 June 2025.

122 See, in this regard, Joerges and others, above n 8.

The Politics of Standardising Ethics. The IEEE Initiative and the Governance of AI

by **Simone Casiraghi and Niels van Dijk ***

Abstract: Although scholars have discussed the role of both ethics and technical standards in AI regulation, the recent creation of technical standards on AI ethics has been under-discussed. We explore this gap by asking two related questions: 1) How does ethics change through standardisation? 2) What should be the mutual roles for risk producers, assessors and bearers in the use of ethical standards for governing AI risks? Our case study is the Institute for Electrical and Electronic Engineers (IEEE) 7000-2021, part of the IEEE 7000 series, and its potential interplay with the AI Act requirements (AIA; Art. 40-41). We follow approaches from Science and Technology Studies (STS) and social sciences studies of risk, which allows us to study standards 1) as an exemplary case of the phenomenon of the AI ethification and institutionalisation of ethics, 2) which is increasingly framed in terms of (ethical or value) risks to be minimised and managed. We aim to show that ethics standards, while they promise to offer a more responsible way to govern AI, transform ethics into an engineering requirement modelled on the procedures, language and logic of operationalisation of standardisation. As a result, IEEE ethics standards suffer from traditional challenges related to representation, accountability, and enforcement. We, therefore, argue that there is a need for 1) a division of powers between risk producers and "ethical" assessors of risk who define acceptable "ethical" thresholds; 2) alternative, dissenting voices in standardisation working groups, especially civil society or consumer organisations that are often de facto excluded from these exercises.

Keywords: Technical standards; ethics; artificial intelligence; representation; risk governance; AI regulation

Recommended citation: Simone Casiraghi and Niels van Dijk, The Politics of Standardising Ethics. The IEEE Initiative and the Governance of AI, 17 (2026) JIPITEC 36 para 1.

A. Introduction: Standards and the Governance of the EU

1 "Soft law" or non-binding initiatives have been gaining momentum since at least 2018 as more flexible alternatives to traditional ways of regulating AI technologies. At least two examples of non-binding initiatives have played a central role in the AI debate: 1) ethics, as self-regulation, in the form of guidelines, lists of principles or frameworks and 2) technical standards. Both instruments are claimed to play a role beyond, on top of or in alternative to the law, allowing to boost innovation while at the same time preventing harm to individuals and benefiting society at large.

2 Resorting to ethics or technical standards as "soft law" or non-binding initiatives in the governance of digital technologies is not a new phenomenon.[1] The combination of these two tools, however, with the creation of standards *on* the ethical aspects of AI systems, is unprecedented.[2] The resort to ethics in

* Simone Casiraghi is Guest Professor and Postdoctoral researcher at the Law, Science, Technology and Society Group (LSTS) at the Vrije Universiteit Brussel (VUB). Niels van Dijk is Associate Professor of Legal Philosophy and Legal Sociology at VUB-LSTS.

1 Mariachiara Tallacchini, 'Governing by Values. EU Ethics: Soft Tool, Hard Effects' (2009) 47 Minerva 281; Annalisa Volpato, 'The Legal Effects of Harmonised Standards in EU Law: From Hard to Soft Law, and Back?' *The Legal Effects of EU Soft Law* (Edward Elgar Publishing 2023).

2 While standards of ethics are new, they can be considered a sub-type of process-oriented standards and share similarities with standards intended to have social benefits, e.g. the ISO 26000:2010 or ISO 14000 series on environmental management. In fact, the ethics involved in these standards

AI governance has already been largely criticised by scholars,[3] while the novelty of Standard Developing Organisations (SDOs) influencing how ethical aspects of AI (including values and fundamental rights) are understood and operationalised has so far been under-discussed.

3 In this article, we focus on the Institute for Electrical and Electronic Engineers (IEEE) 7000-2021 standard, part of the IEEE 7000 series which is claimed to be the first series on ethical standards in history, and on its potential interplay with the AI Act (AIA) requirements (Art. 40-41). The AIA follows the logic of the New Legislative Framework (NLF) in relation to high-risk AI systems (Chapter III),[4] a regulatory technique in EU Law that stemmed from the difficulty in achieving the internal market and removing technical barriers to trade within the EU. Since the adoption of directives intended to harmonise technical requirements in the 1980s was too slow, the European Commission opted for a system in which technical requirements would be created by standardisation bodies rather than being included in legislation. This can be considered a case of co-regulation where market actors are entrusted with the implementation of EU law, i.e. rulemaking is outsourced to the private sector, which creates and approves these regulatory instruments, by EU institutions.[5] Following this logic, the AIA is meant to leave "broad principles" of legislation (e.g. the essential requirements for high-risk AI systems) to EU institutions while assigning technical issues regarding the implementation of the law to standardisation bodies.

4 However, the NLF has focused, so far, primarily on developing standards for the protection of health and safety, while the AIA also seeks to protect fundamental rights, requiring a broader understanding of the rule of law and human rights law,[6] and more generally politically charged and value-laden issues. According to the European Commission, the idea of the NLF is to draw a line between political and technical tasks. On the one hand, the legislator makes political choices, i.e. the EU defines "essential requirements" as precise as possible in legislation, to ensure products traded in the EU meet high-level health, safety, and environmental requirements. On the other hand, standard organisations provide high-quality technical specifications and are not given any political powers.[7] However, this distinction in practice is not that neat. Essential requirements in the AIA leave many open questions about how to operationalise fundamental rights and other ethical principles or values to standard organisations, whose members, organisational infrastructure and procedures differ from traditional rulemaking.

5 Aiming to explore the novelty and consequences of standards on ethics, we ask the following research questions:

- How does ethics change through standardisation? How are ethical values transformed through the standardisation process?
- What should be the mutual roles for risk producers, assessors and bearers in the use of ethical standards for governing AI risks?

6 To answer these questions, we follow approaches from Science and Technology Studies (STS) and social sciences studies of risk, which allow us to study standards from two interrelated viewpoints. First, we consider AI ethics standards as a case study of the broader phenomenon of "ethification".[8] STS scholars have studied ethics not as an academic discipline or philosophical endeavour (i.e. what ethics is), but in

is not really about the ethical behaviour of those who make the system, i.e. engineers and policy makers who act ethically in their profession. The goal is not to define ethical actions per se, but to help an organisation manage ethical issues, through a series of checklists in the design and development phase.

3 Niels van Dijk, Simone Casiraghi and Serge Gutwirth, 'The "Ethification" of ICT Governance. Artificial Intelligence and Data Protection in the European Union' (2021) 43 Computer Law & Security Review 105597; Paul Nemitz, 'Constitutional Democracy and Technology in the Age of Artificial Intelligence' (2018) 376 Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences 1; Ben Wagner, 'Ethics as an Escape from Regulation: From Ethics-Washing to Ethics-Shopping?' in Mireille Hildebrandt (ed), *Being Profiled. Cogitas Ergo Sum* (Amsterdam University Press 2018).

4 However, other chapters of the Act depart from this model, introducing different regulatory approaches for prohibited, limited-risk, and general-purpose AI. These parts of the Act will be out of the scope of this article.

5 Carlo Colombo and Mariolina Eliantonio, 'Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?: Case C-613/14 James Elliot Construction Limited v. Irish Asphalt Limited, EU:C:2016:821' (2017) 24 Maastricht Journal of European and Comparative Law 323, 324.

6 Mélanie Gornet and Winston Maxwell, 'The European Approach to Regulating AI through Technical Standards' (2024) 13 Internet Policy Review; Alessio Tartaro, 'Value-Laden Challenges for Technical Standards Supporting Regulation in the Field of AI' (2024) 26 Ethics and Information Technology 72.

7 European Commission, "Vademecum on European Standardisation in Support of Union Legislation and Policies. Part I: Role of the Commission's Standardisation Requests to the European Standardisation Organisations" (2015) 9.

8 Niels van Dijk and Simone Casiraghi, Law, Morality and Digital Ethics (Edinburgh University Press 2025); van Dijk, Casiraghi and Gutwirth (n 3).

its institutionalised form.[9] This concerns what (self) proclaimed ethicists claim ethics is (discursive angle) and what ethicists do in specific sites that are set up do deal with ethics-related tasks (institutional angle).[10] Standards on ethics are a fascinating case because ethics, for the first time, enters the arena of technical standards, with its procedures, language and engineering-like logic of operationalisation.

7 Secondly, social sciences studies of risk help us frame governance questions about risk, which are relevant to our case because institutionalised ethics, in its various forms, from research ethics protocols[11] to ethical guidelines, is also framed in terms of risks to be minimised and managed. These questions pertain to e.g. who gets to decide what the acceptable "ethical" level of risk of AI systems is, or how much bias such a system can have. Social sciences studies of risk have long criticised the notion of risk as an allegedly neutral scientific object, which instead presupposes several normative assumptions.[12] Beck argues that risk governance has become a central political issue that involves a triad of different kinds of actors. The main opposition is between the actors who generate the risks ("risk producers") and those public or private bodies that are responsible for assessing and mitigating such risks ("risk assessors"). However, risks, much like wealth, are unevenly distributed in society. Their consequences often fall on more vulnerable and marginalised individuals or communities ("risk bearers"), who nonetheless tend to have little to no say about how the risks are assessed.[13]

8 Beck critically addresses the core logic of the NLF. While legislators describe the general program of dealing with risks, the power of determining risks and defining thresholds of acceptability is left to experts in standardisation bodies.[14] It is experts in these bodies who decide, and design accordingly in the standard, what constitutes a high or low risk, how severe certain harms to individuals and society should be considered, and also what are the thresholds after which a risk becomes unacceptable.

9 The separation assumed by the NLF between political and technical tasks hardly fits the content of essential requirements in the AIA that leave many open questions about how to "technically" operationalise politically charged matters such as fundamental rights and other ethical values. This separation[15] becomes even more problematic if there is no parallel division of power between those who produce (risk producers) and those who decide on how to evaluate risks (risk assessors). Both activities are left to standardisation bodies, which often lack robust mechanisms to ensure that the interests of industry do not prevail over those of the people affected by AI risks in society (risk bearers).

10 We focus on IEEE 7000-2021, now also adopted by ISO,[16] because, among the IEEE's ethical standards, it is the one which makes the most explicit references to "ethics", "ethical theories", "ethical principles" or "ethical values".[17] However, the scope of our analysis is not merely IEEE 7000-2021. We use this standard as an exemplar case[18] to make more

9 Simone Casiraghi, "Anything New under the Sun? Insights from a History of Institutionalized AI Ethics" (2023) 25 *Ethics and Information Technology*; Ulrike Felt and others, *Taking European Knowledge Society Seriously* (Publications Office of the European Union 2007); Nina Frahm and Kasper Schiølin, "Toward an 'Ever Closer Union'" (2023) 15 *STS Encounters*; Kjetil Rommetveit, "(How) Can You Build Ethics into Artificial Intelligence?" (2025); Tallacchini (n 1) 281.

10 In this regard, ethics in its institutionalised form, e.g. in the case of ethics advisory groups, has been already criticised by us and other STS scholars, also in other fields like life sciences, as a form of "de-politicising" expertise, for its lack of representativeness and checks and balances.

11 Simone Casiraghi and Niels van Dijk, 'Ethics Reviews in the European Union. Implications for the Governance of Scientific Research in Times of Data Science and Artificial Intelligence' (2024) 16 Law, Innovation and Technology 101.

12 Felt and others (n 9).

13 In Beck's writings, the most vulnerable risk bearers are low-income communities placed close to dangerous waste facilities, nuclear reactors or industrial plants. In the context of AI, vulnerable risk bearers are children, racial and ethnic minorities and individuals with disabilities. See Gianclaudio Malgieri and Maria-Lucia Rebrean, "Vulnerability in the EU AI Act: Building an Interpretation" [2024] SSRN Electronic Journal.

14 Ulrich Beck, 'From Industrial Society to the Risk Society: Questions of Survival, Social Structure and Ecological Enlightenment' (1992) 9 Theory, Culture and Society 97, 107.

15 Sheila Jasanoff, *The Fifth Branch. Science Advisers as Policymakers* (Harvard University Press 1990).

16 As ISO/IEC/IEEE 24748-7000:2022.

17 Despite being under the umbrella of the Global Initiative, not all standards explicitly refer to "ethics" or draw on moral philosophy and academic AI ethics discussions. Examples are IEEE 7002 and 7010, whose main concepts are data protection and human well-being respectively, and were therefore excluded from this article.

18 To date, to the best of our knowledge, there are no independent academic, industry or NGO-led empirical studies documenting the practical application of the standard analysed in this article. Methodologically, a meaningful empirical assessment would require access to confidential internal evaluations and compliance documentation, implying a distinct, *ad hoc*, ethnographic research design beyond the scope of this article. Publicly cited "success cases" are primarily produced by the IEEE itself and provide limited transparency. For example, a pilot project with Wiener Stadtwerke (municipality of Vienna) resulted in certification of an AI-based email classification system, but the assessment report has not been made public (only slides and a blog post). Failure cases, which would

general considerations that would also apply to standardisation efforts of EU bodies like CEN-CENELEC, where other concepts such as fundamental rights, fairness, trustworthiness, transparency[19] and bias are used.

11 The structure of the article will be as follows. In the next section, we introduce the IEEE initiatives on the standardisation of ethics and zoom in on the origins and content of the IEEE 7000-2021 standard. Section C will move to the critical part from three perspectives. First, despite their proclamations, it shows how doubtful it is that ethical standards will manage to foster compliance with the law. Second, ethical standards suffer from the use of vague and ambiguous terms (such as "values") that might leave room for instrumental interpretation. Third, ethical standards lack mechanisms to ensure a representative participation of risk bearers in their working groups. Section D analyses the overlaps and gaps with the AIA and shows how the same critiques apply to the standardisation of AI in the EU. In the conclusion, we will wrap up and provide avenues for further research.

B. Mapping: IEEE 7000-2021 and Its Relationship with the EU AI Act

12 The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems (A/IS),[20] launched in April 2016, had two key milestones:[21] 1) the publication of a main document called "Ethically Aligned Design" (EAD)[22] and 2) the creation of several standard working groups, inspired by this document, aiming to produce the IEEE 7000 standards series, i.e. a group of twelve standards addressing ethical issues of AI.[23]

13 The EAD aims to guide the community of technologists and designers of AI, as well as educators and policymakers, on the ethical aspects of AI systems. The document includes a mixture of high-level ethical principles and "classical ethics", metrics to measure them and practical recommendations to operationalise ethics that can also offer guidance for standardisation activities, certification, design or (legal) regulation of AI.[24]

14 The second milestone of the initiative, i.e. the IEEE 7000 standards series, proclaims to be the first series of standards in history that explicitly focus on societal and ethical issues of a specific set of technologies, and that the IEEE 7010-2020 is the first ethics standard ever produced.[25] The series covers several topics, such as design, privacy and data governance of children, or nudging, and aims to operationalise ethical principles included in the EAD document.

I. A Standard for Addressing Ethical Concerns During Systems Design

15 Before moving to the content of IEEE 7000-2021, a brief overview of how standards are developed at IEEE is needed to understand who gets to participate in each project and how one can contribute.[26] Any IEEE standard typically follows a procedure which consists of six stages.[27] In stage 1, an idea or concept to be standardised is developed and approved. In stage 2, a "working group" (WG) is recruited to start drafting the standard. This stage is important to ensure the representativeness of different interests. Working groups can be very wide, even up to 1000 people,[28] participation may be open or restricted to IEEE members depending on the type of standard, and each participant may have different expertise and carry a different interest, such as producer, user, seller or regulator. Each WG is then divided into subgroups and assigned specific tasks.[29]

16 Stage 3 culminates with the draft of the standard achieved via consensus through meetings and discussions. When it comes to voting for certain

be particularly informative, are not publicly available. The absence of publicly available empirical case studies is therefore not merely a gap in the literature, but itself a key aspect of the problems that our analysis seeks to highlight.

19 Charlotte Högberg, 'Stabilizing Translucencies: Governing AI Transparency by Standardization' (2024) 11 Big Data & Society 1.

20 This is the term chosen by IEEE, but, from now on, we will simply use the term "AI" for consistency with the EU framework.

21 See https://standards.ieee.org/wp-content/uploads/import/documents/faqs/gieais-faq-11.22.2020.pdf

22 Institute of Electrical and Electronics Engineers (IEEE), Ethically Aligned Design. A Vision for Prioritizing Human Well-Being with Autonomous and Intelligent Systems (2019).

23 Rommetveit (n 9).

24 Institute of Electrical and Electronics Engineers (IEEE) (n 22) 2.

25 This is what some of the people involved in the initiative claim, despite there being at least one precedent in British Standard (BS) 8611:2016 on "Robots and robotic devices. Guide to the ethical design and application of robots and robotic systems".

26 To know more about the internal procedures at IEEE, such as voting, see the IEEE Constitution and Bylaws document available at https://ieee-org.widen.net/s/xcmfjhtrv2/ieee-constitution-and-bylaws

27 See https://standards.ieee.org/develop/

28 Matthew Linares, "Industry Standards Won't Give Artificial Intelligence a Conscience" openDemocracy (2019) 1.

29 In P7000 (the WG for IEEE 7000-2021), it was decided on 4 subgroups: ethics, system and their stakeholders, risk and process.

motions (e.g. on administrative issues, the creation of a subgroup, or changes in the document) each voting member has a say.[30] Examples of discussions revolved around which principles should be included in the standard,[31] the use of the word "ethics" as opposed to "value-based"[32] or the role of human rights.[33] Once the draft is finalised, it is submitted to various boards that review it: the so-called balloting process (Stage 4) to finalise the document, the review by the IEEE SA Standards Board Review Committee for final approval (Stage 5) and possible revisions or corrections after the standard is published (Stage 6).

17 The aim of the 7000-2021 standard is to support organisations in "creating ethical value" through system design of all kinds of products and services, and more specifically "to strengthen their value proposition and avoid value harms".[34] Simply put, the standard provides a process by which engineers can include considerations on ethical values (including risks) throughout the research and development stage of a product. The process aims to find a balance of long-term values such as sustainability, privacy, fairness, social responsibility and accountability with short-term time and budget constraints.

18 IEEE 7000-2021 consists of two main stages.[35] The first stage is the "concept exploration stage", which includes two phases, i.e. 1) concept of operations and context exploration process and 2) ethical values elicitation and prioritisation process. The first focuses on how a system is expected to operate from the user's perspective, its context(s) of use and which stakeholders are involved throughout the system's lifecycle. This stage also includes a legal feasibility analysis, which addresses pertinent laws and regulations, due diligence, accountability, consultation with regulatory bodies and ownership, but these questions are not meant to be exhaustive. In the second, stakeholders identify, with the help of ethical theories (i.e. virtue ethics, consequentialism and deontology), values affected by the system. Values are then prioritised (or ranked) and scrutinised.[36] To support this first stage, Annex A provides a philosophical basis for value concepts, i.e. Material Value Ethics and the writings of e.g. the 20th Century phenomenologist Max Scheler (1874-1928) and Nikolai Hartmann (1882-1950).[37] According to this approach, to simplify, values are not individual preferences or opinions, nor characteristics of things, but are "given" (directly perceivable or accessible, in a phenomenological way) *a priori*, and materialise in a given context, similar to Platonic ideas. This theory aims to help not only to recognise values but also to provide criteria to rank them.[38] In particular, higher values are those that persist the most, that are less extensible or divisible, less founded through other values, provide more satisfaction to humans and are less dependent on a specific bearer.[39] Annex G includes a list of typical ethical values, such as autonomy, care, control, fairness and privacy.[40] The aim of this annex is to compare values elicited in the process with a list of common ethical values to avoid inadvertent gaps. The table assigns "related values" and "opposing values" to each value (e.g. privacy is related to anonymity, and "opposed" to transparency and inclusiveness).

19 The second stage is called the development stage. It includes two more phases: 1) the "ethical requirements definition process"[41] 2) the "ethical risk-based design process". The first phase asks the organisation to "formulate" high-ranked ethical values as system requirements that specify how the values are operationalised in the technological

30 Usually, membership and voting rights are granted based on attendance, e.g. a non-member becomes a non-voting member by attending one meeting, a non-voting member becomes a voting member by attending 2 of the last 4 meetings and voting membership is granted to those participants attending the first meeting of a newly chartered WG. The opposite also applies, e.g. a non-voting member becomes a non-member by not attending any of the last 2 meetings, and a voting member who has not attended at least 2 of the last 4 meetings becomes a non-voting member.

31 From the minutes of 7/03/2017: "Ethical principles in P7000 was also a strong topic in the responses. [...] Several points were noted on principles; it is hard to maintain an ethical standard when you say pick and choose what suits you, should meet minimal requirements. Principles guide behavior. Principles evolve. Sarah [Spiekermann] noted the two principles she sees resonating with the group; We are committed to a value-based design and We make design decisions fully visible (transparent)."

32 From the minutes of 25/09/2017: "Carolyn [Nguyen, from Microsoft] and others outlined that P7000 should [not] use the word "ethical" all the time, but "value-based" design; [it should] avoid "moral" language in the standard".

33 From the minutes of 25/09/2017: "Human rights were discussed and the question how human rights could enter the standard. As part of principles? As part of baseline values?"

34 Institute of Electrical and Electronics Engineers (IEEE), 'IEEE Standard Model Process for Addressing Ethical Concerns during System Design' (2021) 9.

35 ibid 35.

36 ibid 14, 15, 30.

37 ibid 53; Sarah Spiekermann and Till Winkler, "Value-Based Engineering for Ethics by Design" [2020] SSRN Electronic Journal 4.

38 Institute of Electrical and Electronics Engineers (IEEE) (n 34) 55.

39 ibid 56.

40 ibid 69.

41 ibid 43.

system. An example provided is how full-body scanners at the airport should protect the value of privacy. The value of privacy should be formulated first as general rules such as "The system shall protect the privacy of body images of scanned passengers" and later into explicit value-based systems requirements, e.g. "The system shall display images of suspected contraband metal, plastic, ceramic, and explosive items positioned on a generic body outline".[42]

20 The second phase, the "ethical risk-based design process", is not very detailed but builds on risk management requirements of other IEEE standards (e.g. ISO/IEC/IEEE 16085:2021), including general risk management, risk identification, risk analysis and risk mitigation. A crucial phase is the identification of risks "associated with the feasibility of implementing the design", which should be performed "in consultation with stakeholders".[43] This phase concerns the determination of the kinds of risk that will (or will not) be taken into consideration during the process. Differently from the AIA, risks in IEEE 7000-2021 are not directly risks of harm to the health, safety or fundamental rights of natural persons, but risks that the value-based system requirements are not realised in the system (which, in turn, might cause risks to individuals, but could also be reputational risks to the organisation and its shareholders). Another important process phase relates to the definition of thresholds, including the determination "whether risks to value-based requirements are at a level within the system design that stakeholders find tolerable (acceptable) without the need for further treatment".[44]

21 Later in the process, however, it is noted how "this standard does not prescribe any specific design solutions. [...] This level of detail (e.g., the use of millimeter wave technology or X-ray backscatter technology for scanning) is left to other domain-specific standards and the competence of the designers".[45] This means that it is up to AI designers *within* the organisation and other *technical* standards to define more precise risk identifications and risk acceptability thresholds.

C. Three Critiques on (Un)ethical Standardisation Activities

22 To recap, 1) the IEEE initiative on ethics is an unprecedented combination of ethics and standards for AI governance and 2) such an initiative might be influential for the EU standardisation activities for the AIA's chapter on high-risk systems, which follows the NLF logic. According to this logic, the European Commission assumes there is a boundary between political and technical(-ethical) issues: on the one hand, the legislator defines high-risk AI systems' "essential requirements" in legislation, on the other, SDOs define technical specifications based on such requirements. This model would prevent standard organisations from having "political powers".[46] This assumption, however, seems to collide with the idea of ethics as an object of standardisation.

23 STS authors have already shown how such a clear distinction between politics and science, between Research and Innovation agendas and research projects, or between policymaking and the advice of expert groups, is highly problematic.[47] Making ethical standards inevitably requires value choices (e.g. choosing a value-based instead of principle-based approach, choosing material value ethics as a guiding theory or adopting certain criteria to rank values) on contestable political issues in settings that are considered "purely" technical and dominated by an engineering and business-oriented mindset.[48]

24 Especially through the NLF, a problem of division of powers becomes manifest. The design of risk assessment methods and the way they are conducted are operationalised in (several) standardisation bodies. In such bodies, those who produce these risks (i.e. organisations using AI systems) have a main say about how they are managed, assessed and mitigated.

25 The following sub-sections will zoom in on some of the recurring challenges in the standard-making of AI ethics from three perspectives: compliance, vagueness and representativeness, which especially points to several limitations of the standard IEEE 7000-2021 that we have just analysed.

I. The Role of Standards in Achieving Compliance

26 One of the major promises of IEEE ethical standards, and standards in general, is that they would help a company or organisation to ensure (or foster) compliance with legislation. This links with the NLF idea of "presumption of conformity" highlighted in the previous section. For example, IEEE standards are claimed to clarify what is at stake and explain requirements in layman's terms since they show

42 ibid 54.
43 ibid 48.
44 ibid 48.
45 ibid 55.
46 European Commission (n 7) 9.
47 Jasanoff (n 15); Felt and others (n 9); Tallacchini (n 1).
48 Johann Laux, Sandra Wachter and Brent Mittelstadt, "Three pathways for standardisation and ethical disclosure by default under the European Union Artificial Intelligence Act" (2024) 53 Computer Law & Security Review 105957.

"good faith efforts beyond minimal levels of compliance", they can reduce a company's liability and they show that organisations are ready to adhere to future laws and regulations.[49] While the potential of IEEE 7000-2021, for e.g. operationalising Art. 9 AIA requirements, may sound very appealing, especially for the EU legislator and for EU companies, at a closer look it is difficult to see how IEEE could achieve "more than compliance".

27 In IEEE 7000-2021, although the standard also claims to "engage with the original spirit of laws, human rights and other social values in the specific context of a system's use",[50] the legal requirements and fundamental rights angle are underdeveloped in the process. The only reference to legal requirements in the process is the legal, social and environmental feasibility study and analysis guidelines.[51] This part only includes six very broad questions with little guidance on how to answer them[52] and gives no indications of how specific any reply to the legal questions should be. Although it makes sense to stay at an abstract level in such a standard, given its international scope *qua* jurisdictions, this guidance still sounds too broad, and there are no safeguards in place in case the feasibility analysis concludes that the AI system does not comply with the law.

28 Moreover, the questions are mostly about ownership and accountability (questions 1 and 4), therefore privileging the focus on the organisation developing or deploying AI systems rather than on (the fundamental rights of) individuals affected by them. This way, following ethical standards becomes more related to the public perception of the organisation rather than to the (negative) effects on individual users.[53]

29 Additionally, there is no explicit reference to other legal frameworks relevant to AI, such as data protection law, human rights law or the legal frameworks that specifically deal with privacy, transparency, and algorithmic bias. It is up to the organisation to find out which "local, regional, national, and international regulatory bodies should be consulted or enhanced to evaluate a full 360 view of the SOI's [System Of Interest] legal responsibilities" (question 2), as well as "what are the laws regulating current and future income streams related to SOI design" (question 5).

30 In short, what emerges from IEEE 7000-2021 is a narrow vision of compliance with the law, that mostly looks at organisations and internal stakeholders (and their accountability) rather than at the consumer end (such as fundamental rights, including e.g. data subject rights), and instead of going "beyond mere compliance", or achieve "presumption of conformity" under EU law, it may not even get close to it. This is because, while there is an overlap in terms of scope, the legal part of the IEEE 7000-2021 process seems very generic and marginal, with only 2 pages annexed in the entire document. Yet, it is difficult to complete, since there is little guidance (e.g. what are the laws regulating the system?) and organisations could be tempted to skip the process or do it superficially.

II. Interpretative Vagueness and Ambiguity of Ethical Requirements

31 Not only the legal requirements but also the content of AI ethical standards has been considered vague and/or ambiguous,[54] because of the very same matter such documents are meant to standardise. Turning values or fundamental rights (e.g. privacy) into standards leaves much room for interpretation,[55] depending on the interests at stake, regarding e.g. risk thresholds and mitigation measures to address such risks.

32 In IEEE 7000-2021, this critique mostly pertains to the concept of value and its value-based, or "design for values" approach.[56] Value-based ethical approaches for AI and IT systems more generally, including e.g.

49 Daniel Schiff and others, 'IEEE 7010: A New Standard for Assessing the Well-Being Implications of Artificial Intelligence' *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (2020).

50 Institute of Electrical and Electronics Engineers (IEEE) (n 34) 14.

51 ibid 62.

52 The only explanation is that "[t]he legal questions can be applied to already enacted laws and regulations, as well as to cross-jurisdiction and cross-functional considerations and to potential laws and regulation, that may affect the SOI [system of interest], its users and other stakeholders, and the broader international context". ibid.

53 Niels van Dijk, Raphaël Gellert and Kjetil Rommetveit, 'A Risk to a Right? Beyond Data Protection Risk Assessments' (2016) 32 Computer Law & Security Review 286.

54 Tambiamba Madiega, 'EU Guidelines on Ethics in Artificial Intelligence : Context and Implementation' (2019) 9.

55 Ine van Zeeland and Jo Pierson, 'How Standards Co-Shape Personal Data Protection in the European Banking Sector' *2021 IEEE European Symposium on Security and Privacy Workshops* (2021).

56 Jeroen van den Hoven, Pieter Vermaas and Ibo van de Poel (eds), *Handbook of Ethics, Values, and Technological Design. Sources, Theory, Values and Application Domains* (Springer 2015).

value-sensitive design (VSD),[57] values in design[58] and Participatory Design,[59] from which IEEE 7000-2021 takes explicit inspiration,[60] have been criticised for different reasons.[61] The core idea of these criticisms is that the vagueness and ambiguity of the way values are formulated can lead to instrumentalisation, and there is a risk that engineers use values that are unprincipled or unbound.[62]

33 Firstly, there is a definitional problem, i.e. that the concept of value and its realisation is left undetermined or underdeveloped.[63] In its origins in the early 1990s, VSD did not define the word "value" explicitly, focusing on broader areas of concern such as human dignity or welfare.[64] However, VSD has always aimed to focus on moral values in information technology,[65] and specifically around human-computer interaction, such as trust, autonomy or privacy.[66] In IEEE 7000-2021, however, it is less clear which values are considered. Some of them, which are treated in other IEEE standards, are explicitly excluded (i.e. health, security and safety).[67] Annex G includes typical ethical values and Max Scheler's material value ethics is taken as a reference point and combined with scholarly work on values in system design. This is an original combination, and particularly worth attention since in other cases there is rarely a philosophical foundation for these works.[68] However, the values mentioned are characterised only briefly, which might result in reducing them to mere preferences and wishes of stakeholders.[69]

34 The definitional problem is aggravated by the issue of possible value conflicts. The solution of IEEE 7000-2021 is to adopt value ranking criteria[70] which follow the classic trade-off strategy, such as privacy vs. security. Trade-off is a well-known strategy for VSD approaches (e.g. safety vs. efficiency),[71] but it has been criticised for being overly simplistic. Problems that are presented as mathematical, quantifiable and objective are in fact value-laden. The risk of these discourses is that political conflicts and power asymmetries are reframed as mere technical ones.[72] For example, the language of the trade-off privacy vs. security is often enforced in contexts (cultures, organisations) which systematically favours security (e.g. to defend travellers from terrorist attacks), while both privacy and security could be enforced without loss on either of the two. Moreover, some conflicts of values cannot even be solved in terms of trade-offs, for example, when two or more values are "incommensurable", i.e. they cannot be expressed or measured on a common scale.[73]

35 Finally, besides the problem regarding *how* to make a choice, there is also the issue of *who* ultimately makes the choice or who interprets. VSD and IEEE 7000-2021 only ease value conflicts; they do not solve them. A choice still needs to be made, but it is often unclear who makes it and on what basis. In IEEE 7000-2021, it is not specified who makes the final decision on how to prioritise these competing values, either stakeholders or designers/engineers, and, in the

57 Batya Friedman and Peter Kahn, "Value Sensitive Design: Theory and Methods" (2002) University of Washington Computer Science Technical Reports 1.

58 Mary Flanagan, Daniel C Howe and Helen Nissenbaum, 'Embodying Values in Technology: Theory and Practice' in Jeroen van den Hoven and J Weckert (eds), *Information Technology and Moral Philosophy* (Cambridge University Press 2008); Helen Nissenbaum, 'Values in Technical Design' *Encyclopedia of Science, Technology and Ethics* (Macmillan 2005) lxvi.

59 Douglas Schuler and Aki Namioka, *Participatory Design: Principles and Practices* (Lawrence Erlbaum Associates 1993).

60 Spiekermann and Winkler (n 37).

61 Wessel Reijers and others, 'Methods for Practising Ethics in Research and Innovation: A Literature Review, Critical Analysis and Recommendations' (2018) 24 Science and Engineering Ethics 1437; Noëmi Manders-Huits, 'What Values in Design? The Challenge of Incorporating Moral Values into Design' (2011) 17 Science and Engineering Ethics 271, 277.

62 Janet Davis and Lisa P Nathan, 'Value Sensitive Design: Applications, Adaptations, and Critiques' in Jeroen van den Hoven, Pieter Vermaas and Ibo van de Poel (eds), *Handbook of Ethics, Values. and Technological Design* (Springer 2015).

63 Manders-Huits (n 61); Ibo van de Poel, "Embedding Values in Artificial Intelligence (AI) Systems" (2020) 30 Minds and Machines 385.

64 Davis and Nathan (n 62) 14.

65 Batya Friedman, 'Value Sensitive Design' *Berkshire encyclopedia of human-computer interaction* (Berkshire Publishing Group 2004).

66 Similar approaches like "Design for X" focus also on instrumental values like maintenance, reliability and cost. See Raymond Holt and Catherine Barnes, "Towards an Integrated Approach to 'Design for X': An Agenda for Decision-Based DFX Research" (2010) 21 Research in Engineering Design 123.

67 Institute of Electrical and Electronics Engineers (IEEE) (n 34) 13.

68 van Dijk, Casiraghi and Gutwirth (n 3).

69 Manders-Huits (n 61) 281.

70 Institute of Electrical and Electronics Engineers (IEEE) (n 34) 55.

71 Ibo van de Poel, 'Values in Engineering Design' in Anthonie BT Meijers (ed), *Handbook of the Philosophy of Science* (North-Holland 2009).

72 Simone Casiraghi, J Peter Burgess and Kristoffer Lidén, 'Ethics and Border Control Technologies' in J Peter Burgess and Dariusz Kloza (eds), *Border Control and New Technologies. Addressing Integrated Impact Assessment* (Academic and Scientific Publishers 2021) 90.

73 Ibo van de Poel and others, *Ethics, Technology and Engineering: An Introduction* (Wiley-Blackwell 2011) 182.

former case, which group of stakeholders. Choosing one or the other group could lead, in principle, to very different results.

36 In sum, standards are meant to reduce uncertainty and provide stability, but the vagueness of their content makes such standards even more uncertain and open to (instrumental) interpretation. In IEEE 7000-2021 this concerns values considered and their definitions, how to rank them and relate them to classic ethical theories (if deemed necessary).

III. Representativeness and Participation

37 Regarding representativeness, the IEEE has developed rules to ensure the inclusiveness and representativeness of its WGs and avoid certain interests prevailing over others, but it is doubtful whether these rules work in practice to avoid overrepresentation of the industry as the main risk producer. The reality is that people from civil society organisations (e.g. trade unions), who represent the interests of the most affected risk bearers in society, are *de facto* excluded by these bodies, and not because they lack initiative, but because they would have to pay high fees[74] and join meetings in expensive (and possibly exotic)[75] places.[76] On top of this, doing ethics in standardisation bodies is still unaffordable even among smaller companies: only big companies can afford, economically and timewise, to have ethics experts on their payroll.[77]

38 An additional problem related to representativeness lies in the articulation of the concept of stakeholder involvement in the process described by the standard. "Stakeholder" is considered a key concept in the process of IEEE 7000-2021[78] and it plays a role in three crucial phases, i.e. value elicitation and prioritisation, ethical requirements definition process and ethical risk-based design process. The idea is that a group of stakeholders as wide as possible[79] should be involved early in the project to ensure the broadest scope of values and ethical requirements for the system. However, while it is recognised that the "users" are a group of stakeholders that is "intrinsic to ethical risk-based design", a business mentality in identifying stakeholders is prevalent: "[a]s for any engineering design effort, the interests of the project owners or the organisation's top management along with the system architects and designers are typically predominant. The acquirers for a custom-built system, or whoever identifies the needs to be translated into requirements, such as business or market analysts, and portfolio managers, or product line managers, are also considered as major stakeholders".[80] There is a thorough level of granularity when it comes to describing these "internal" stakeholders,[81] but the same cannot be said for the external stakeholders and especially the consumer end or civil society. IEEE 7000-2021 only provides a few examples of groups of vulnerable people or risk bearers who could be specifically affected by AI systems and would need to be involved in the process.

D. Overlaps and Gaps Between AIA and IEEE 7000-2021

39 As the AIA moves toward implementation, IEEE 7000-2021 may offer concrete methods that align with the AIA's essential requirements. Both from the point of view of IEEE and the European Commission, there are large overlaps between the work of IEEE on ethics standards and the role technical standards play in the EU AI regulation.

74 For example, for IEEE membership to be a voting member of a WG or to be part of the balloting process.

75 This does not apply to the IEEE WG analysed in this article (where most meetings took place remotely, possibly due to the Covid-19 pandemic), but it is not rare in IEEE. See for instance the planned session of IEEE 802.15 in places like Hawaii, Thailand and Bahamas: https://grouper.ieee.org/groups/802/15/pub/Meeting_Plan.html

76 See the discussion during the 2019 Computers Privacy and Data Protection Conference (CPDP) panel, organised by IEEE and moderated by Paul Nemitz, titled "Technical standards on ethics and/or regulation?" The intervention of Ponce del Castillo, researcher and lawyer at the European Trade Union Institute, at minute 52, is about where civil society organisations are sitting in standardisation bodies. At the same conference panel, Alessandro Guarino, researcher and information security professional working at some CEN-CENELEC standards, talks about the lobby problem that affects standard organisations. Video available at https://www.youtube.com/watch?v=Cf7xcRzOwvI

77 Jacob Metcalf, Emanuel Moss and Danah Boyd, 'Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics' (2019) 82 An International Quarterly 449, 457.

78 Institute of Electrical and Electronics Engineers (IEEE) (n 34) 27.

79 Examples provided by the document are "Human beings using the system, organizations representing human beings using the system, supporters, developers, producers, trainers, maintainers, disposers, acquirers, supplier organizations, and regulatory bodies". Institute of Electrical and Electronics Engineers (IEEE) (n 34) 21.

80 ibid.

81 See how, for instance, on 20/12/20, Lewis Gray from Abelia Corporation proposed to include explicitly "profit" as an ethical value and to include the notion of "shareholder" as distinct from stakeholder. The vote failed (14 no and 1 yes).

40 According to Art. 40, organisations can follow a harmonised standard to comply with the requirements of the AIA or can follow common specifications[82] adopted by the Commission rather than interpreting the essential requirements set out in the regulation.[83] Providers do not have to follow such standards, but, in practice, they are cheaper and safer for producers to follow. In fact, conformance with standards or common specifications is a means to reduce compliance burdens for AI providers.[84]

41 CEN and CENELEC are important actors in the AIA since they can be mandated by the Commission, on a formal request, to develop harmonised standards,[85] following the procedures established by regulation 1025/2012. In 2023, the European Commission asked CEN and CENELEC to focus on "ten concrete aspects of AI", including risk management, transparency, human oversight and the conformity assessment procedure. This led to the creation of the Joint Technical Committee (JTC21).[86] The references of the standards published by the JTC21 are published in the Official Journal of the European Union (OJEU) once the Commission services evaluate them positively to satisfy the standardisation request.[87] Only standards published in the OJEU can provide operators with a relevant legal "presumption of conformity" with the legal requirements of the EU harmonisation legislation in question.[88] However, there are appropriate agreements[89] between European Standardisation Organisations (ESOs) and International Standardisation Organisations (such as ISO and IEC), which ensure that international standards can be proposed as European harmonised standards in response to a standardisation request.[90]

42 Contrary to the IEEE, the emphasis of JTC21's AI standardisation on "ethics" has been rather marginal. Considering the emphasis the Commission had put on the ethics of AI right before the AIA proposal,[91] the word "ethics" or "ethical" does not play a central role in the text of the AIA.[92] However, the essential requirements of Chapter III (Articles 8-15), which form the core of AI standardisation work, are based on the "seven requirements" developed by the European High-Level Expert Group on AI in their ethical guidelines.[93]

43 Still, although the IEEE is an international organisation and US-based, and therefore not part of European Standard Organisations (ESOs)[94] defined in Regulation 1025/2012,[95] the work of IEEE might still

82 Art. 3 (28) AIA defines "common specification" as "a document, other than a standard, containing technical solutions providing a means to comply with certain requirements and obligations established under this Regulation".

83 Art. 41 AIA discusses "common specifications" in cases where harmonised standards may not exist or may not apply. See Michael Veale and Frederik Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act' (2021) 4 *Computer Law Review International* 97, 105.

84 Mark McFadden and others, *Harmonising Artificial Intelligence: The Role of Standards in the EU AI Regulation* (Oxford Information Labs, 2021) 7 https://oxcaigg.oii.ox.ac.uk/wp-content/uploads/sites/11/2021/12/Harmonising-AI-OXIL.pdf.

85 Veale and Borgesius (n 83) 104.

86 See https://publications.jrc.ec.europa.eu/repository/handle/JRC139430?utm_source=substack&utm_medium=email

87 Stefano Nativi and Sarah De Nigris, 'AI Watch: AI Standardisation Landscape: State of Play and Link to the EC Proposal for an AI Regulatory Framework' (Joint Research Centre, 2021) 7 https://data.europa.eu/doi/10.2760/376602.

88 Regulation (EU) 1025/2012 sets the general rules regarding the functioning of the standardisation system, including the procedure for issuing standardisation mandates (Art. 10). After citation in the Official Journal of the European Union, harmonised standards are considered EU law.

89 For instance, the Vienna (1991) & Frankfurt (2016) agreements signed between CEN-CENELEC, ISO and IEC to avoid duplication of standards at international and European level (Available respectively at https://isotc.iso.org/livelink/livelink/fetch/2000/2122/3146825/4229629/4230450/4230458/01__Agreement_on_Technical_Cooperation_between_ISO_and_CEN_(Vienna_Agreement).pdf?nodeid=4230688&vernum=-2 and https://assets.iec.ch/iecwebsite/partners/IEC-CENELEC_Frankfurt_Agreement%7B2016%7D.pdf). This is particularly relevant since IEEE 7000 has been adopted, in its form analysed in this article, by ISO/IEC as ISO/IEC/IEEE 24748-7000, available at https://www.iso.org/standard/84893.html

90 IEEE 7000-2021 has been adopted by ISO-IEC as ISO/IEC/IEEE 24748-7000:2022. Available at https://www.iso.org/standard/84893.html.

91 van Dijk, Casiraghi and Gutwirth (n 3).

92 The word rarely appears in the text. Article 40 refers to ethical reviews required by the EU for testing high-risk systems outside regulatory sandboxes; Article 95 and Recitals 7, 27 and 165 refer to the AI High-Level expert group guidelines.

93 High-Level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI (2019) 15 https://data.europa.eu/doi/10.2759/346720.

94 IEEE is nevertheless one of the relevant SDOs having a formal recognition by international treaties and regulations or SDOs participating in the bi-annual Global Standards Collaboration, which also includes ETSI, CEN-CENELEC, ISO/IEC and ITU-T. See Nativi and De Nigris (n 87) 9.

95 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

affect, at least in principle, the EU standardisation practices on AI. In fact, it is in the EU's strategic interest to cooperate with a broader network of standard organisations.[96] Also, many key actors from EU-based organisations are part of IEEE initiatives[97] and IEEE is related to the EU in several ways.[98]

44 IEEE 7000-2021 might be relevant for the AIA in terms of scope (rather broad in terms of technologies considered, across a variety of sectors) and horizontal nature[99] of the regulation, and therefore it could provide the technical specifications that support AI systems operators to achieve and demonstrate compliance with the legal requirements.[100] The EC's Joint Research Centre[101] has deeply focused on IEEE initiatives and their interplay (including potential misalignments) with the AIA in their report on the AI Standardisation landscape.[102] The report concludes that the IEEE 7000 series covers most of the requirements for high-risk systems under the AIA.[103] In particular, IEEE 7000-2021 is considered "very relevant" for the work of the JTC21 especially regarding risk management, making it relevant for adoption at the EU level.[104] The design-oriented focus of IEEE 7000-2021 provides a unique perspective that can be useful for AI providers of high-risk systems that want to integrate risk considerations early in the development process.[105] An example is the risk management system in Art. 9 of the AIA.[106] The risk approach of Art. 9 takes account of the consequences of high-risk AI systems for individual persons and their health, safety and fundamental rights (the risk bearers), or for society more generally.

45 We have already pointed out the limitations of IEEE 7000-2021 that might hinder the possibility that it becomes adopted as a harmonised standard in the EU under the AIA. However, the critiques in the previous section do not simply apply to the IEEE case, but have also implications for other EU standardisation activities, even if IEEE 7000-2021 will never be adopted by CEN-CENELEC. To begin with, the role of standards in achieving compliance remains problematic because many standards adopted by CEN-CENELEC are transpositions of international standards (ISO-IEC),[107] which could also have a generic jurisdictional focus, therefore glossing over the specificities of the EU legal framework.[108] The Commission has already admitted, for example, how the approach of international standardisation bodies on risk "does not align with the AI Act, for instance on the notion of risk, which is understood by ISO [in e.g. ISO/IEC 42001:2023] as organisational risk, and not as risk to health, safety and fundamental rights, such as in the AI Act".[109]

46 There will also be similar problems of interpretative vagueness and ambiguity with other contested (ethical) concepts that need to be standardised for the AIA. This leaves ample room for interpretation, such as AI transparency[110] or privacy.[111]

47 As for the problem of inclusiveness, a 2025 report of the Corporate Europe Observatory shows how the EU standardisation efforts for AI are dominated by Big Tech.[112] 55% of the JTC21 members come either from corporations or consultancy, with nearly a quarter of corporate representatives coming from US industries, such as Microsoft, Amazon and Google. Only 16% come from academia/think tanks

Decision No 1673/2006/EC of the European Parliament and of the Council, *OJ L 316, 14.11.2012, p. 12–33.*

96 McFadden and others (n 84) 39.

97 For instance, Sarah Spiekermann.

98 For instance, the IEEE has an EU-based headquarters in Vienna, where an initiative was carried out with the municipality. IEEE also uses terminology inspired by EU initiatives on AI, such as "trustworthy" and "human-centric" AI.

99 This means that AIs across sectors are subject to the same risk assessment criteria and legal requirements. A vertical approach would, by contrast, apply only to a specific AI application or sector.

100 Nativi and De Nigris (n 87) 7.

101 The EC's science and knowledge service that aims to provide evidence-based scientific support to the European policymaking process.

102 Josep Soler Garrido and others, Harmonised Standards for the European AI Act (Joint Research Centre, 2024) https://publications.jrc.ec.europa.eu/repository/handle/JRC139430.

103 ibid 33.

104 ibid 29.

105 ibid.

106 And, to a lesser extent, Art. 10 (data and data governance) and Art. 13 (transparency and provision of information to users.

107 A 2023 report from CEN-CENELEC shows that 35% of CEN's standards were direct transpositions of ISO's, and 81% of CENELEC standards were adoptions of IEC's. Available at https://www.cencenelec.eu/media/CEN-CENELEC/European%20Standardization/Documents/IC/global_outreach_dec2023.pdf

108 Athena Christofi and others, 'Erosion by Standardisation' in Maria Tzanou (ed), *Personal Data Protection and Legal Developments in the European Union* (IGI Global 2020).

109 In a response to a letter by the Corporate Europe Observatory, available at https://corporateeurope.org/sites/default/files/2025-01/response-CEO-8Jan.pdf

110 Högberg (n 19).

111 Kjetil Rommetveit and Niels van Dijk, "Privacy Engineering and the Techno-Regulatory Imaginary" (2022) 52 Social Studies of Science 853.

112 Available at https://corporateeurope.org/en/2025/01/setting-rules-their-own-game-how-big-tech-shaping-ai-standards

and 9% from civil society.[113] The report claims that such a vast representation allows industry players to play several "tactics" in the interest of light-weight standards that are difficult to enforce, such as insisting on transposing international standards or influencing national delegations. In other words, while risk bearers are suffering the most severe consequences of risks stemming from AI systems, they are hardly represented and have a chance to speak in standardisation bodies and assessment processes that aim to manage such risks.[114]

48 Also, the issues about the articulation of the concept of stakeholder involvement go beyond the case of IEEE. These processes of IEEE 7000-2021 are modeled on the phases of other international standards which might influence EU activities, such as ISO/IEC/IEEE 12207:2017,[115] called "stakeholder needs and requirement definition".[116] This problem seems endemic for other examples of institutionalisation of ethics of AI initiatives in the EU, such as the AI High-Level Expert Group.[117]

E. Concluding Remarks: The Need for a Division of Powers

49 To conclude, this article discussed the politics of ethical standards in the governance of AI. After a brief introduction, we mapped the IEEE initiative on the standardisation of AI ethics, providing a quick overview of the standardisation process at IEEE and of the content of the standard IEEE 7000-2021. Afterwards, we focused on three main criticisms of this standard, which are nevertheless applicable to similar ongoing standardisation efforts in EU bodies that are crucial for the AIA implementation: compliance, vagueness and representation.

50 We started the article with two research questions. First, we asked how ethics changes through standardisation and, more specifically, how ethical values transform through the standardisation process. After a close analysis of IEEE 7000-2021, we have shown how ethics (including ethical values but also concepts such as privacy or transparency) becomes an "engineering" requirement modelled on the procedures, language, logic of operationalisation of standardisation and risk. In IEEE 7000-2021, for instance, ethical values are identified and ranked and later formulated as system requirements. However, it remains challenging to translate ethical concepts into such logical specifications, and the same challenge will apply to the EU harmonised standards for the AIA.

51 The semantic openness of concepts such as values and fundamental rights contrasts with the need for unambiguous and precisely formulated system requirements.[118] Additionally, the risk-based approach is central in IEEE, like in the AIA, but "risk", as well as stakeholders meant to evaluate it, for IEEE are intended more from the organisation's perspective than for individuals. This discrepancy is related to the difference between the concepts of risk to the organisation vs. risk as an individual's legal and political rights.[119] In the first case, the main concern is the possible damage to the reputation or trust in the organisation that an infringement might cause. Ethics standards are, in this case, mainly aimed at boosting the image of an organisation to the public's view.[120] In the second case, instead, the focus

113 It must be said that there is no official list of JTC21, so the method used by the Corporate Europe Observatory is based on self-reporting. In particular, a search was conducted for variations of the term "JTC21" on LinkedIn to identify individuals who claimed to be involved in this standardisation committee.

114 On this line, the European Ombudsman initiated an inquiry on the inclusiveness and transparency of JTC21 efforts in September 2025. The inquiry addresses a complaint that the Commission has not required CEN-CENELEC to publish information about the members of the JTC21, the minutes of meetings and other documents of the working group, and has failed to ensure a balanced representation of interests for the process of developing the standards. See European Ombudsman, Inquiry into complaint 1974/2025/MIK against the European Commission (2025) https://link.europa.eu/GGp9mT.

115 International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and Institute of Electrical and Electronics Engineers (IEEE), 'Systems and Software Engineering — Software Life Cycle Processes'.

116 Institute of Electrical and Electronics Engineers (IEEE) (n 34) 52.

117 Simone Casiraghi and Niels Van Dijk, "Constituting a Sovereign European Identity through AI Ethics. A Critical Exploration" in Luca Marelli and others (eds), *Project Europe. The Making of European Digital Innovation, Policy and Society* (Edward Elgar 2025).

118 Kjetil Rommetveit, Alessia Tanas and Niels van Dijk, "Data Protection by Design: Promises and Perils in Crossing the Rubicon Between Law and Engineering" in Marit Hansen and others (eds), *Privacy and Identity Management. The Smart Revolution* (Springer International Publishing 2018); Niels van Dijk and others, "Right Engineering? The Redesign of Privacy and Personal Data Protection" (2018) 32 *International Review of Law* 230.

119 Van Dijk and others (n 53) 3.

120 Ansgar Koene and others, 'IEEE P70xx, Establishing Standards for Ethical Technology', Proceedings of KDD'18, ExCel (2018). This is not only an issue for IEEE. Other important standard organisations, like ISO, are primarily bodies for coordinating standardisation efforts by private businesses, although some of their members are governmental organisations like national standardisation bodies. Here, standards are primarily adopted by industry

is on perceptions of individual right holders, which are the basis for (legal) claims to human rights.[121]

52 Second, the more normative question of the article pertained to what the mutual roles for risk producers, assessors and bearers in the use of ethical standards for governing AI risks should be. As we are witnessing a convergence of two modes of governance of AI (institutionalised ethics and standards), we also see a shift from (mostly) public to (mostly) private actors in shaping the form these standards should take. Having more budget and personnel, Big Tech players are having a larger influence on the creation of the standards, including in European SDOs. Flexible procedures and loose rules for representation may allow industrial players to steer the agenda and direction of standards, as well as the application of the AIA more broadly, leaving little room for concerns raised by other societal interests.

53 We observed that the politics of risk involves a triad of actors, i.e. risk producers, risk assessors and risk bearers. What often happens in standardisation bodies is that there is no distinction between risk producers and assessors, that is, those who produce risks are also those who evaluate them, or at least risk producers have a strong hand in the standardisation and assessment process. Through their presence in standardisation bodies, risk producers can determine which risks are considered acceptable and if/how they can be mitigated. At the same time, little room is given to risk bearers, who are suffering the most consequences of such risks and who are de facto excluded from standardisation bodies and assessment processes.

54 For these reasons, we argue that there is a need for a division of powers between risk producers and "ethical" assessors of risk. Once the normative dimension of risk is opened up, those who are affected by the risks (risk bearers) should also have a chance to "speak". In relation to standards, this means that alternative, dissenting voices and disciplinary diversity are also needed in standardisation working groups, especially civil society or consumer organisations that are often excluded de facto from these exercises.[122] For the AIA, a possible recommendation is to require standards, instead of asking the AI providers to set ethical thresholds themselves (e.g. how much bias is acceptable) as is the case in IEEE 7000-2021, to ask providers to disclose "relevant documentation, including test results, impact assessments, transparency disclosures and explanations".[123] This is just an example, and such disclosure would exceed the current reporting requirements of the AIA, but it might as well empower people or institutions, closer than providers to the context in which the AI system is actually used, to co-decide whether a system is "ethically" acceptable.[124]

55 Finally, we want to conclude by stressing that, in this article, we dealt more with the standardisation of ethics and the politics of standardisation, leaving the question of the ethics of standardisation unaddressed. The meta-question about the ethics of standardising ethics would require separate work, but we agree with the idea that standards are intertwined with moral philosophical questions that require serious scrutiny, such as "questions about who we are, how we want to live, and what is the right thing to do. The answers to these sorts of questions may incorporate expert knowledge, since that knowledge can offer new opportunities for action. But an expert claiming to have clear answers to these questions should be viewed with considerable suspicion".[125]

Acknowledgments

This research was made possible through funding from the Vrije Universiteit Brussel's Strategic Research Program 'Articulating Law, Technology, Ethics, Politics: Issues of Enforcement and Jurisdiction of EU Data Protection Law under and beyond the General Data Protection Regulation (ALTEP-DP)' (SRP54).

representatives for the benefit of the industry (but there can be some side positive effects).

121 van Dijk and others (n 53) 9.

122 Beck (n 14) 61.

123 Laux and others (n 48) 12.

124 Since similar issues may arise in other regulatory contexts, such as in Asia or the United States, comparative work across jurisdictions also represents an important direction for future research.

125 Lawrence Busch, *Standards. Recipes for Reality* (MIT Press 2011) 285.

The Role of the European Commission in the Control of Harmonised Standards Under the AI Act and the Challenges of "Opacity"

by **Mariolina Eliantonio** *

Abstract: This article examines the role of the European Commission in the European standardisation process, with a specific focus on the development of harmonised standards under the AI Act. Such standards, historically used in product safety regulation, are developed through a peculiar co-regulatory model (the New Legislative Framework). Thereby, private bodies, the European Standardisation Organisations (ESOs), draft technical standards that, once controlled by the Commission for compliance with the underlying legislation and subsequently referenced in the Official Journal, acquire binding public law relevance through the presumption of conformity. The latter allows products which respect the referenced harmonised standards to enter the internal market without the need for additional proof of compliance with the legislative requirements.

While this model has long raised rule of law concerns, the AI Act presents an unprecedented challenge by requiring ESOs to design standards that not only safeguard health and safety but also protect fundamental rights—an inherently vague, value-laden, and contested task. The article argues that the Commission's control over draft standards is the last crucial "public law check" in the European standardisation process. By retracing the evolution of this control before and after the CJEU's James Elliott ruling and interpreting the Standardisation Regulation historically, systematically, and teleologically, the contribution demonstrates that Commission oversight is a fundamental step in the process which the Commission ought to carry out with adequate depth, so as to prevent the transfer of indirect normative power to private actors.

Against the backdrop of delays in AI standardisation and pressure to operationalise the AI Act swiftly, the article warns against a "rubber stamping" approach and highlights the heightened importance of meaningful Commission scrutiny when standards affect not only market functioning but also the protection of fundamental rights and the very legitimacy of the EU legal order.

Keywords: AI Act, harmonised standards, European Commission, fundamental rights, New Legislative Approach

Recommended citation: Mariolina Eliantonioi, The Role of the European Commission in the Control of Harmonised Standards Under the AI Act and the Challenges of "Opacity"I, 17 (2026) JIPITEC 49 para 1.

A. Introduction

1 The New Legislative Framework (NLF) – a peculiar mode of co-regulation dating back from the 80s – is increasingly expanding its reach from product safety to digital regulation, as it is currently foreseen as a regulatory technique in, amongst others, the Cyber Resilience Act,[1] the Data Act,[2]

* Mariolina Eliantonio, Professor of European and Comparative Administrative Law and Procedure, Maastricht University;

1 Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) OJ L 29.10.2024.

2 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules

the Chips Act[3] as well as the AI Act.[4] The co-regulatory core of this technique resides in a partnership between the EU co-legislators, which draft legislation foreseeing essential health and safety requirements for products and services, the European Standardisation Organisations (ESOs), in charge of drafting detailed technical specifications on how to meet those essential requirements, and the European Commission, which is mandated to draft standardisation requests to the ESOs and publish a reference to the produced standards in the Official Journal, rendering them "harmonised standards". As extensively argued in respect of the use of the NLF, there are many and clear benefits in relying on technical standards and co-regulation in the EU internal market and beyond. The use of the NLF technique has allowed overcoming the slowness of the removal of trade barriers by means of legislative action and, through the coordination with the global standard-setting bodies, the interconnection between the EU and the global markets.[5] In the words of the European Commission, "[S]tandardisation has played a leading role in creating the EU Single Market. Standards support market-based competition and help ensure the interoperability of complementary products and services. They reduce costs, improve safety, and enhance competition".[6] The same is true also for digital regulation: in the fast-paced world of technology, leaving technical details to experts while not overburdening law-makers ensures that the developed solutions remain up-to-date with scientific and technical developments as well as a high degree of interoperability, leading to undeniable trade benefits.[7]

2 At the same time, the public law relevance of the process of European standardisation and the tensions which it produces in respect of basic tenets linked to the rule of law have been at the core of much of the scholarly debate in the past years.[8] When the New Legislative Framework met the AI Act, the well-known "quandaries"[9] (is European standardisation in line with the *Meroni* doctrine of delegation of powers?[10] To which extent are harmonised standards judicially reviewable by the Court of Justice of the European Union (CJEU)?[11] Should the process of European standardisation respect general principles of administrative law, such as the duty to give reasons?[12]) have taken a whole new dimension.

3 Indeed, the AI Act - in its Article 40 - has entrusted the ESOs with the "mission impossible" to draft technical standards for high-risk AI systems which would ensure compliance with not only health and safety requirements, but also the fundamental rights of individuals.[13] The mission seems to be "impossible" because the AI Act remains overly

on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) OJ L 22.12.2023.

3 Regulation (EU) 2023/1781 of the European Parliament and of the Council of 13 September 2023 establishing a framework of measures for strengthening Europe's semiconductor ecosystem and amending Regulation (EU) 2021/694 (Chips Act) OJ L229/1.

4 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) OJ L 12.7.2024.

5 H Schepel, *The Constitution of Private Governance – Product Standards in the Regulation of Integrating Markets*, (Hart, 2005); J Pelkmans, 'The New Approach to Technical Harmonization and Standardisation' (1987) 25 Journal of Common Market Studies 249.

6 European Commission, 'Standardisation policy' (*European Commission*) <https://single-market-economy.ec.europa.eu/single-market/goods/european-standards/standardisation-policy_en> accessed March 24th 2026.

7 PA Earls Davis and R Schmidt, 'Standardised Bias? The Role – and Limits – of European Standards Bodies in the EU's Artificial Intelligence Act' (*Internet Policy Review*, 24 July 2025) <https://policyreview.info/articles/news/bias-european-standards-bodies> accessed March 24th 2026.

8 E.g. H Schepel, 'The New Approach to the New Approach: The Juridification of Harmonised Standards in EU Law' (2013) 20 Maastricht Journal of European and Comparative Law 521; R van Gestel and HW Micklitz, 'European Integration through Standardisation: How Judicial Review Is Breaking Down the Club House of Private Standardisation Bodies' (2013) 50 Common Market Law Review 145; M Eliantonio, 'Private Actors, Public Authorities and the Relevance of Public Law in the Process of European Standardisation' (2018) 24 European Public Law 437; M Eliantonio and M Medzmariashvili, 'Hybridity Under Scrutiny: How European Standardization Shakes the Foundations of EU Constitutional and Internal Market Law' (2017) 44 Legal Issues of Economic Integration (special issue).

9 See Kanevskaia in this special issue who recalls the 'quandary' which the process of European standardisation has generated for the European legislator.

10 E.g. L Senden, 'The Constitutional Fit of European Standardization Put to the Test' (2017) 44 Legal Issues of Economic Integration 337; M Medzmariashvili, 'Delegation of Rulemaking Power to European Standards Organizations: Reconsidered' (2017) 44 Legal Issues of Economic Integration 353.

11 M Eliantonio, 'Judicial Control of the EU Harmonized Standards: Entering a Black Hole?' (2017) 44 Legal Issues of Economic Integration 395; C Tovo, 'Judicial Review of Harmonized Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU Law' (2018) 55 Common Market Law Review 1187.

12 M Gnes 'Do Administrative Law Principles Apply to European Standardization: Agencification or Privatization?' 44 (2017) Legal Issues of Economic Integration 367.

13 See on this point Oliva in this special issue.

vague on which fundamental rights are at stake, how to control compliance, and how to balance possibly conflicting fundamental rights.[14] The vague, value-laden, requirements of the AI Act and the conundrum it generates for ESOs (needing to translate deeply contextual and politically sensitive concepts into universal procedures) has not gone unnoticed.[15]

4 What is more, technical standards themselves hide complex value judgements and require evidence which is often incomplete, uncertain, or context-dependent, generating a further "mission impossible" also for regulatees.[16]

5 The fact that the new EU Standardisation Strategy acknowledges that standards deal not only with technical components "but also incorporate EU core values and interests",[17] does not render the mission less "impossible", but rather brings to the fore the one actor which – by reason of its very existence – is supposed to pursue (in the process of European standardisation and beyond it) the public interest: the European Commission.

6 According to Article 17 TEU, the Commission is tasked with pursuing the general public interest in the EU. In the context of the process of European standardisation, the Standardisation Regulation specifically foresees that the Commission must check the compliance of the standards drafted by the ESOs with its initial request.[18] In light of the vagueness of the requirements set in the AI Act, of the crucial role assigned to the ESOs (ie private bodies) to assess technical standards against the equally opaque concept of fundamental rights, and of the relevant consequences which the law assigns to standards which – after approval of the Commission – become "harmonised", all eyes are on the European Commission.

7 The Commission is – in other words – the last "public law check" before a privately developed norm acquires public law relevance, namely through the presumption of conformity. In the context of the AI Act, for the reasons discussed above, this last check acquires, it can be argued, a heightened importance vis-à-vis, for example, "the making available on the market of electrical equipment designed for use within certain voltage limits".[19]

8 The aim of this contribution is to examine the specific juncture in which standards drafted by the ESOs upon a request by the European Commission under the Standardisation Regulation are at a crossroad of becoming (or not) harmonised standards through the publication of a reference to them in the Official Journal. The choice of which road to take is made by the European Commission which needs to assess whether the standards comply with its initial request and the underlying legislation.

14 On this see M Ho-Dac, 'Considering Fundamental Rights in the European Standardisation of Artificial Intelligence: Nonsense or Strategic Alliance?' in K Jakobs (ed), *Joint Proceedings EURAS & SIIT 2023* (Verlag Günter Mainz 2023); M Cantero Gamito and C T Marsden, 'Artificial intelligence co-regulation? The role of standards in the EU AI Act' 32 (2024) International Journal of Law and Information Technology, eaae011; A Mantelero, 'The AI Act: A Realpolitik Compromise and the Need to Look Forward' in I Spiecker Döhmann, L Schertel Mendes and R R Campos (eds), *Digital Constitutionalism* (Nomos 2025) 311; M Gornet, 'The European approach to regulating AI through technical standards' (2023) hal- 04254949v1<https://hal.science/hal-04254949v1>. From the side of civil society, see ANEC, EDRi and EDF, 'The Role of Standards and Standardisation Processes in the EU's Artificial Intelligence (AI) Act' (*EDRi*, May 2022) <https://edri.org/wp-content/uploads/2022/05/The-role-of-standards-and-standardisation-processes-in-the-EUs-Artificial-Intelligence-AI-Act.pdf> accessed 30 March 2026; Frederico Oliveira da Silva and Kasper Drazewski, 'Regulating AI to Protect the Consumer: Position Paper on the AI Act' (*BEUC*, 7 October 2021) <https://www.beuc.eu/sites/default/files/publications/beuc-x-2021-088_regulating_ai_to_protect_the_consumer.pdf> accessed 30 March 2026. See also the report by H-W Micklitz (commissioned by BEUC and ANEC), *The Role of Standards in Future EU Digital Policy Legislation - A Consumer* Perspective, especially 95 and ff.

15 A Tartaro, 'Value-laden challenges for technical standards supporting regulation in the field of AI' 26 (2024) Ethics and Information Technology 1. The author argues that "[I]t is impossible to technically specify what constitutes an *acceptable* level of risk, an *appropriate* level of accuracy, and a *commensurate* level of human oversight". Similarly, Peter Alexander Earls David and Rebecca Schmidt consider that "[B]ias and (fairness) in AI is a highly contested concept, even (or perhaps especially) in technical fields". P A Earls Davis and R Schmidt, 'Standardised bias?' (n 7).

16 See on this point Tartaro, Obnasca and Panai in this special issue.

17 European Commission, 'An EU Strategy on Standardisation: Setting Global Standards in Support of a Resilient, Green and Digital EU Single Market' (Communication) COM (2022) 31 final, 4.

18 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 [2012] OJ L 316/12, Article 10(5).

19 Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits [2014] OJ L 96/357.

9 The argument advanced here is that, if the Commission does not exercise a sufficient degree of control over the draft standards, it will contribute to the "opacity" of the regulatory architecture supporting the implementation of the AI Act, thereby ultimately undermining the legitimacy of this very architecture.[20] In order to build this argument, the notion of "opacity of the law", in the particular in the sense of "opacity of the legal provisions" will be employed.

10 A legal provision becomes opaque "when it contains technical terms or expressions, incorporated into the text on the advice of experts, which escape the understanding of the legislators".[21] In turn, this opacity affects the legitimacy of the legal provisions because legislators incorporate into legal provisions technical terms or expressions whose content lies beyond their own knowledge and understanding. The content of the "law" thus ends up being determined by technical bodies that operate outside the democratic-constitutional purview. In this way, "[T]he epistemic authority granted to experts [...] turns into an indirect normative power, removed from the institutional control mechanisms that are proper to a state governed by the rule of law".[22]

11 When applied to the process of European standardisation, these considerations would translate into the following: if the Commission accepts to publish in the Official Journal a reference to a technical standard without understanding and controlling its content and its consequences, it would end up affording an indirect normative power to the ESOs which would be in breach of the rule of law.[23] The question thus arises as to the scope and intensity of control which the Commission exercises and – from the point of view of avoiding "opacity" in the sense presented above – ought to exercise on the draft standards produced by the ESOs.

12 In order to elucidate both the positive and the normative question just enunciated, this article shall re-trace the evolution of this control before and after the CJEU's *James Elliott* ruling[24] and, through a historical, systematic, and teleological interpretation of the provisions of the Standardisation Regulation, discuss the scope and intensity of the Commission's control over harmonised standards, including the ones connected to the AI Act.

B. The Commission's Role in Controlling Draft Standards: A Long and Winding Road

I. Setting the Scene: Harmonised Standards, the AI Act and the Role of the Commission

13 On 22 May 2023, the European Commission issued a standardisation request to the ESOs to deliver standards in support of the AI Act.[25] CEN and CENELEC have been tasked to draft a first set of standards, which should reflect the generally acknowledged state of the art to prevent and minimise risks to health, safety, and fundamental rights of persons, as guaranteed in the Charter of Fundamental Rights as well as in relevant applicable EU law.[26]

14 Once drafted, according to Article 10(5), second sentence, and (6) of the Standardisation Regulation, the Commission is both obliged and entitled to check whether the mandated harmonised standards meet the requirements of the standardisation request, prior to publication of the reference in the Official Journal. Indeed, according to the former provision, the Commission together with the ESOs "shall assess the compliance of the documents drafted by the European standardisation organisations with its initial request". Pursuant to Article 10(6), "[W]here a harmonised standard satisfies the requirements which it aims to cover and which are set out in the corresponding Union harmonisation legislation, the Commission shall publish a reference of such harmonised standard without delay in the Official Journal of the European Union".

15 The scope and intensity of the Commission's control over the produced harmonised standards is not mandated or specified by the Standardisation

20 The legitimacy challenges in this context have been masterfully summarized by A Tartaro, 'Regulating by standards: current progress and main challenges in the standardisation of Artificial Intelligence in support of the AI Act' (2023) 1 European Journal of Privacy Law and Technology, 147.

21 D Canale, 'Quando gli esperti creano diritto: deferenza, opacità, legittimità", (2022) Analisi e Diritto, 157, 159. For similar considerations in English (but more focused on the role of courts in situations of "opacity"), see D Canale, 'The Opacity of Law: on the Hidden Impact of Experts' Opinion on Legal Decision-Making', 40 (2021) Law and Philosophy, 509.

22 D Canale, 'Quando gli esperti creano diritto' (n 21), 166.

23 See to this effect, the CJEU's *Meroni* ruling. Case 9-56, *Meroni & Co., Industrie Metallurgiche, SpA v High Authority of the European Coal and Steel Community* ECLI:EU:C:1958:7.

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

25 European Commission, 'Commission Implementing Decision of 22 May 2023 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' C (2023) 3215 final.

26 Ibid., Annex II, 2.

Regulation and has been the subject matter of some debate in the aftermath of the *James Elliot* ruling in which the CJEU held that "harmonised standards form part of EU law".[27] The ruling established that the CJEU has jurisdiction to interpret harmonised standards and, in general, opened a debate on the side of both the European Commission and the ESOs[28] on the reach of public law guarantees over the process of European standardisation.

16 Both the silence on this matter in the Standardisation Regulation and the controversy sparked by the *James Elliott* ruling warrants an examination of the rules concerning the practice of the Commission in the control of harmonised standards, a matter, as will be shown in the next section, still of great contention.

II. How It Started and How It Is Going: The Evolution of the Role of the Commission Through the Standardisation Regulation

17 Traditionally, the publication of references to harmonised standards was not preceded by any substantive control by the Commission.[29] In a 1998 Report from the Commission it was actually explicitly stated that "no positive decision is required by which authorities approve the standards".[30] The same is reiterated in a 2002 guidance document where it was stated that "ex-ante control of the technical work by the legislation does not take place".[31] At the same time, rather contradictorily, that same guidance document provided that "the European legislator *maintains control* of the final results as he needs to publish the references of these standards in the OJ in order for the standards to have legal effect (presumption of conformity)".[32] (emphasis added)

18 The fact that the Commission was effectively not controlling the process is supported by the fact that, as noted by Schepel, in its most common form in early New Approach Directives, the Commission could initiate an *ex post* objection procedure if it thought that a harmonised standard did not (or no longer) respect the health and safety requirements foreseen by the underlying legislation.[33] Indeed, the relevant clauses read as follows: "Where a Member State or the Commission considers that the harmonized standards [...] do not entirely meet the essential requirements [...] the Commission or the Member State concerned shall bring the matter before the Standing Committee set up under Directive 83/189/EEC, giving the reasons therefor. The Committee shall deliver an opinion without delay. In the light of the Committee's opinion, the Commission shall inform the Member State whether or not it is necessary to withdraw those standards from publication".[34] From a formal perspective, the marginal role of the Commission is also shown by the fact that references to harmonised standards were contained in Commission Communications, non-binding measures published in the C Section of the Official Journal.

19 The 2012 Standardisation Regulation brought about a welcome clarification in this unclear *status quo* by introducing Article 10(5), pursuant to which the Commission must assess whether the standard produced complies with the request on which it is based. Furthermore, according to Article 10(6), the publication of a reference to a harmonised standard in the Official Journal is made condition upon whether the "harmonised standard satisfies the requirements which it aims to cover, and which are set out in the corresponding Union harmonisation legislation". The Regulation therefore highlighted and strengthened the role of the Commission in the standardisation process.

20 The necessity of a form of control is also made clear in the 2015 Vademecum, according to which "specifications delivered by the ESOs in support of Union legislation can never be automatically regarded as complying with the initial request, as this is a political responsibility. As the requesting authority, the Commission will always have to assess compliance with its initial request, in cooperation with the ESOs [...], before deciding to publish the references of a delivered standard in the Official Journal".[35]

27 C-613/14, *James Elliott* (n 24), para 40.

28 CEN and CENELEC, 'CEN and CENELEC Position on the Consequences of the Judgment of the European Court of Justice on *James Elliott Construction Limited v Irish Asphalt Limited*' (*CEN-CENELEC*, 17 May 2017) <https://opil.ouplaw.com/view/10.1093/law-oxio/e246.013.1/law-oxio-e246-document-1.pdf > accessed March 24th 2026.

29 This was noted also by doctrine. H Schepel, *The Constitution of Private Governance* (n 5), 235.

30 See e.g. European Commission, 'Report of 13 May 1998 on efficiency and accountability in European standardisation under the New Approach' COM(1998)291 final, 9.

31 European Commission, 'Methods of Referencing Standards in Legislation with an Emphasis on European Legislation' (Enterprise Guide, European Communities 2002) 9.

32 Ibid.

33 H Schepel, 'The New Approach to the New Approach' (n 8) 529.

34 See e.g. Article 6 of the Simple Pressure Vessels Directive 87/404/EEC [1987] OJ L 220/48. Noted by H Schepel, 'The New Approach to the New Approach' (n 8).

35 European Commission, 'Vademecum on European Standardisation in Support of Union Legislation and Policies: Part I' (Staff Working Document) SWD (2015) 205 final, 9.

21 There is therefore no doubt that – post 2012 – *some* degree of control on the side of the Commission is in line with (and actually required by) the applicable regulatory framework. What remained, however, unclear, is the extent of this control.

III. The Post-James Elliott Scenario and Its Discontents

22 As a consequence of the groundbreaking 2016 *James Elliott* ruling, the Commission felt compelled to take its role in the standardisation process more seriously.

23 In particular, in November 2018, the Commission published a Communication on harmonised standards,[36] where it stated to have "the *obligation* to follow the development process of harmonised standards thoroughly and to assess whether they comply with the requirements set out in harmonised Union legislation and/or standardisation requests in order to ensure that harmonised standards fully comply with the applicable legislation. This does not only include the technical aspects of standards but also other elements of the European Standardisation Regulation, such as whether their development process has been inclusive". It further confirmed that "[I]t is the Commission's intention to fulfil these obligations in a manner which is as swift and efficient as possible".[37]

24 The Commission did not specify (in this document or elsewhere) what precisely its control will entail post-2018. However, several signs show that the Commission wished to be more actively involved in the process of European Standardisation than in the past. In particular, certain concrete changes were brought about. First of all, the Commission ceased to publish references of harmonised standards in the form of a communication in the C series of the Official Journal, but instead in the form of an implementing decision in the L series, reflecting the change in the view of the legal effects of harmonised standards in EU law.[38]

25 Importantly for the purposes of this contribution, the European Commission introduced the Harmonised Standards (HAS) consultants system. HAS consultants are a group of experts provided by a Contractor, currently Ernst & Young, with the purpose of implementing the assessment mechanisms stipulated by the Standardisation Regulation.[39] They have replaced the previous system of so-called NA Consultants (New Approach Consultants), which were managed by the CEN-CENELEC Management Centre but financed via a grant given by the Commission. Although more could (and arguably should) be done in providing more transparency on the role of HAS consultants,[40] these developments do strengthen the impression that the Commission is willing to take more ownership of the process of European Standardisation.[41]

26 This impression is corroborated when looking at the on-going evaluation of the Standardisation Regulation, where reference is made to both of these aspects as a sign of the Commission's efforts to comply with the essence of the *James Elliott* ruling.[42] In particular, the Staff Working Document on the evaluation of the Standardisation Regulation shows that the number of rejections of draft standards rose from 54% to 69%. While this result does not *per se* show a heightened control on the part of the Commission it may give some evidence of a renewed role of the Commission in the process.[43] The same document also states, for example, that there have been "specific cases where the Commission's compliance assessments, supported by HAS consultants, uncover[ed] quality issues that prevent[ed] standards from meeting publication requirements, leading to rejections or the need for further revisions".[44]

27 The depth of the Commission's assessment remains, however, both contested and unclear. The shift towards a supposedly more intensive control has indeed been criticised notably in the Redecker Opinion, commissioned by the German Federal Ministry for Economic Affairs and Energy in view of the Commission's reaction to the *James Elliott* ruling.[45]

36 European Commission, 'Harmonised Standards: Enhancing Transparency and Legal Certainty for a Fully Functioning Single Market' (Communication) COM (2018) 764 final.

37 Ibid., 3.

38 On this A Volpato and M Eliantonio, 'The Butterfly Effect of Publishing References to Harmonised Standards in the L series' (*European Law Blog*, 7 March 2019) DOI: 10.21428/9885764c.3503fd81.

39 Further information on the role envisaged by the Commission for the HAS Consultants can be found in the Tender Specifications published by the Commission itself, Available at https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/tender-details/docs/etender/9845/9845_122895_EN-Tender%20Specifications%20GROW-2021-OP-0016_ENG_V1.pdf .

40 H-W Micklitz, *The Role of Standards in Future EU Digital Policy Legislation* (n 14), 50.

41 For the earlier system CEN/CENELEC see *Guide 15 - Tasks and responsibilities of the New Approach Consultants*, April 2009.

42 European Commission, 'Evaluation of Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European Standardisation' (Staff Working Document) SWD (2025) 171 final, 179.

43 Ibid., 19.

44 Ibid.

45 K Dingemann and M Kottmann, *Legal Opinion on the European System of Harmonised Standards,* Commissioned by the

Considering the trend towards what seemed a tighter form of control, the Opinion argued that this would be incompatible with the Standardisation Regulation and the New Approach paradigm, uncalled for in light of the *James Elliott* ruling, and ultimately as undermining the efficiency and smooth functioning of the standardisation process.[46]

28 Similarly, in a 2023 Report, it has been argued that the post-*James Elliott* approach by the Commission would run against its own established practice, "whereby the technical content of harmonised standards was expressly left to ESOs to decide upon", a practice considered a "core element" of the European standardisation process.[47] Also the move to the use of HAS consultants has been the subject matter of some debate, especially for the alleged limited benefits the new system would deliver and the delays it would generate instead.[48]

29 The next section will unveil why these viewpoints cannot find a basis in the applicable legal framework. Conscious of the hybridity of the model on which European standardisation is founded and of the fact that the delicate public–private balance underlying European standardisation remain normatively important, the argument brought forward is that a substantive control of the Commission over the draft standards is both legally permitted and normatively opportune.

IV. Who Is Afraid of a Tighter Control Over Harmonised Standards?

30 Despite the above-mentioned criticism, a more intense – substantive – control of standards by the Commission before publishing a reference in the Official Journal is fully in line with the legal architecture of European standardisation and, from the perspective of the rule of law, in fact, required to avoid its "opacity". This conclusion can be reached through the systematic, historic and teleological interpretation of the applicable provisions.

31 One argument that has been brought in this context is that Articles 10 and 11 of the Standardisation Regulation would seem to suggest that the Commission should restrict itself to a mere formal control of harmonised standards.[49] A systematic interpretation of the Standardisation Regulation, and in particular the relationship between its Articles 10 and 11, seems, however, to lead to a different conclusion.

32 Article 11 deals with the procedure of formal objection to harmonised standards and it entails the adoption by the Commission of an implementing decision (with the participation of the relevant Comitology committee).[50] In particular, pursuant to this provision, if a Member State or the European Parliament considers that a harmonised standard does not (entirely) satisfy the requirements which it aims to cover, it must inform the Commission. The latter must, after consulting the relevant Comitology committee, decide, to publish, not to publish or to publish with restriction the references to the harmonised standard concerned or, in case the objection is raised after publication, to maintain, to maintain with restriction or to withdraw the references. By contrast, Article 10(6) does not foresee the assistance of a committee and does not make reference to a specific procedure. The difference is procedures would seem to suggest a more limited role for the Commission under Article 10(6) compared to that it would appear to play under Article 11.

33 From these differences, however, and specifically from the circumstance of the presence of the Member States representatives in a consultative role (as foreseen in Article 11), one cannot directly descend any consequence concerning the intensity of the control of the Commission. In both procedures, the decision is ultimately the Commission's, and it is the latter which is entitled to choose how intensively the delivered standards ought to be controlled (regardless of the consultative presence of the Member States authorities).

34 Another criticism brought against a tighter control of draft standards on the part of the Commission is that it would "betray" the aim and spirit of European standardisation. A teleological interpretation of the Regulation would not, however, seem to lead to this result. In particular, and unlike what mentioned in the Redecker Opinion, the main aim of the New Approach is not "to give legislative requirements a concrete form by what of voluntarily applicable, non-binding technical specifications",[51] but to set up, in the words of the Commission, a "public-private-partnership between the Commission and the

German Federal Ministry for Economic Affairs and Energy, 2020.

46 Ibid., 25 to 42.

47 J Baron and P Larouche, *The European Standardisation System at a Crossroads* (Centre on Regulation in Europe Report 2023) 58.

48 Ibid.

49 K Dingemann and M Kottmann, Legal Opinion on the European System of Harmonised Standards (n 45), 28-31.

50 Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers [2011] OJ L 55/13.

51 K Dingemann and M Kottmann, Legal Opinion on the European System of Harmonised Standards (n 45), 32.

standardisation community",[52] the basis of which is enshrined in the peculiar legal consequences arising from the presumption of conformity granted to products which conform to harmonised standards. In light of the relevance of standardisation as a tool to support Union legislation and policies, the Standardisation Regulation stresses the importance that public authorities participate in standardisation at all stages of the development of those standards.[53] Exactly because of the existence of such close partnership, and of the public law consequences arising from the decision of the Commission to publish a reference to a harmonised standard in the Official Journal, a teleological interpretation cannot lead to the conclusion that the control of the Commission over the delivered standards must be limited to a mere formal check.

35 On the contrary, a historical interpretation of the Standardisation Regulation and an examination of the evolution of the regulatory context set up by the New Approach would lead to the opposite conclusion that a more pervasive (and substantive) control of the Commission over harmonised standards before publication is fully compatible with the legislative framework currently in place.

36 As observed in much of the literature discussing technical standards in the EU, the process of European Standardisation has been subject to a progressive "juridification"[54] which has progressively removed it further from the sphere of purely private regulation towards a system of hybrid governance where public authorities play a fundamental role. One of the turning points in this respect can be identified in the Standardisation Regulation. Before its entry into force, the point of departure was that harmonised standards were published in the Official Journal "for information purposes" only.[55] In line with this point of departure, which de-responsabilized the Commission of any form of control, harmonised standards were published as Commission Communications in the C section of the Official Journal.

37 Even before the *James Elliott* ruling, the tide had started to turn with the enactment of the Standardisation Regulation, which instead provides that it is for the Commission to "assess the compliance" of the standards delivered with its initial request prior to the publication of the reference in the Official Journal. Another clear step in the same juridification process is the above mentioned practice, since 2019, to no longer public reference to harmonised standards as non-binding Communications in the C section of the Official Journal, but as implementing decisions in the L section. The legislative and regulatory changes clearly point towards a larger role of the Commission in the process of control of harmonised standards.

38 The same can be concluded when looking at the evolution of the objection procedure. Before the entry into force of the Standardisation Regulation, the objection procedure could be initiated by the Commission or the Member States.[56] The Standardisation Regulation, in its Article 11, gives *Member States* and the *European Parliament* the right to object, but not the Commission itself.

39 This exclusion can only be explained in light of the changed role of the Commission in the process. As observed, indeed, "[A]ccording to the old conception of the act of publication as an act of providing information, the anomaly of the Commission objecting to an act of the Commission could be explained away. Now, however, it seems accepted that the Commission has to take a decision to publish the references, based on a prior assessment: in that case, it is only right and proper that the Commission should not be allowed to object to itself".[57]

40 All of the above suggests that a control of the Commission which extends beyond a mere formal control of the standards but touches also the "substance" (hence the content) of a standard is fully in line with the evolution of the process of European standardisation and the role of the Commission therein.

52 Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, *Harmonised standards: Enhancing transparency and legal certainty* (n 36), 1.

53 Recital 25 of Regulation No 1025/2012.

54 H Schepel, 'The New Approach to the New Approach' (n 8); R van Gestel and HW Micklitz, 'European Integration through Standardisation' (n 8); M Eliantonio and C Colombo, 'Harmonized Technical Standards as Part of EU Law: Juridification with a Number of Unresolved Legitimacy Concerns?' (2017) 24 Maastricht Journal of European and Comparative Law 323.

55 See eg Article 5 of the Low Voltage Directive 73/23/EEC [1973] OJ 1973 L77/29.

56 As noted by Schepel, in its most common form in early New Approach Directives, the relevant clause read as follows: "Where a Member State or the Commission considers that the harmonized standards [...] do not entirely meet the essential requirements [...] the Commission or the Member State concerned shall bring the matter before the Standing Committee set up under Directive 83/189/EEC, giving the reasons therefor. The Committee shall deliver an opinion without delay. In the light of the Committee's opinion, the Commission shall inform the Member State whether or not it is necessary to withdraw those standards from publication". See e.g. Article 6 of the Simple Pressure Vessels Directive 87/404/EEC, OJ 187, L 220/48. H Schepel, 'The New Approach to the New Approach' (n 8), 529.

57 *Ibid*., 530.

41 A final point in support of a substantive control of harmonised standards by the European Commission can be made with respect specifically to the AI Act, through a systematic interpretation of Article 40 in combination with Article 41. While Article 40 mandates indeed ESOs to draft standards which would fulfil the requirements of the AI Act, Article 41 foresees the possibility for the Commission to adopt common specifications through implementing acts, "as fallback solution, so as to ensure that the public interest is served where harmonised standards are absent and insufficient".[58] In particular, the Commission can do so when, amongst other reasons, the relevant harmonised standards insufficiently address fundamental rights concerns or does not comply with the request. When looking at these two provisions together, it can be deduced that their joint reading necessarily implies a control by the Commission on the content of the draft standards, as this control is the condition to trigger eventually the applicability of Article 41 itself.

42 When it comes specifically to the role of the newly introduced HES consultants, it has been considered that their presence is, first of all, unwarranted, "as there is no reason to believe that the opinion of the HAS consultant on the adequacy of the standard is necessarily to be preferred to the collective view of the experts gathered in the ESO technical working group and its decision-making bodies".[59] This view, however, does not take the different roles of the HAS consultants and the experts in the ESOs into account. The ESOs are and remain private organisations, executing admittedly a request coming from a public institution, but at their core still private actors (with clear financial interests in the sale of the standards). The HAS consultants work instead exclusively under the supervision of the Commission: their very *raison d'être* is to support the Commission in the control of harmonised standards. Their role, therefore, while based on expertise as much as that of the ESOs, is fundamentally different and, if the Commission's role in the process is to be taken seriously, their presence constitutes a fundamental step in the public control of the life of a standard towards its mutation into a "harmonised standard".

43 Similarly, while it is true that at the time when the mandate is issued, the technical content of a potential harmonised standard is unknown or at least undetermined, this very circumstance does not logically exclude an external (ie outside the ESOs) control of the draft standards. This would not amount to "second-guessing as to the meaning and interpretation of the mandate in the light of information that was simply not available a priori",[60] but an independent control as to the compliance of the draft standard with the mandate.

C. The Commission's Control of Harmonised Standards Under the AI Act: How to Avoid "Opacity"

44 Having concluded that a substantive control of harmonised standards by the Commission does not violate either the Standardisation Regulation or the New Legislative Framework regulatory paradigm in general, this section analyses the possible intensity of this substantive control. In this context, one could imagine at least two types of substantive control: (i) a more limited one, on the basis of which the Commission would control whether the delivered standard complies with requirements of the underlying legislation, and (ii) more invasive one, on the basis of which the Commission would not only control compliance of the harmonised standard with the mandatory health and safety requirements (as well as fundamental rights under the AI Act), but also whether the specific standard was the most appropriate way to comply with those requirements. The latter – more intense – substantive control would in essence entail that the Commission would end up duplicating the work of the ESOs and eventually substituting its own assessment to that of the ESOs.

45 Despite what has been argued,[61] this latter type of control does not seem what the Commission pledges to carry out in its 2018 Communication, where it "merely" states to intend to control whether harmonised standards "comply with the requirements set out in harmonised Union legislation".[62] An enhanced control of the Commission on the requirements of the harmonisation legislation does not necessarily entail a substantive intrusion in the role of the ESOs. Also from this perspective, therefore, it does not seem that the Commission is intending to perform a stricter control than one which is both allowed *and* required under the current legislative framework. Literature focussing on the AI Act has also specifically called for this type of substantive control, in combination with an increased effort on the part of the Commission to

58 An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market (n 17), 8.

59 J Baron and P Larouche, *The European Standardisation System at a Crossroads* (n 47), 58.

60 Ibid., 59.

61 K Dingemann and M Kottmann, Legal Opinion on the European System of Harmonised Standards (n 45), 39-40.

62 Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, *Harmonised standards: Enhancing transparency and legal certainty* (n 36), 3.

set clear boundaries to ESOs in the standardisation requests.[63]

46 What still remains to be concretised, however, is what that control would entail, not least in the context of the fundamental rights aspects foreseen by the AI Act. The assessment framework used by HAS consultants has been developed by the Commission and can be found in a 2016 document issued by DG GROW.[64] Mindful of its own role, the Commission states that the control under Article 10 of the Standardisation Regulation "contributes to the proper functioning of the single market" and ensures "that the Commission has final control over any assessment work done during the drafting of a harmonised standard".[65]

47 This control process, understood as an "endorsement based on sufficient (but not absolute) certainty that the standard satisfies the relevant legal requirements and other requirements referred to in the relevant standardisation request(s)"[66] comprises three steps. The first step relates to a number of "procedural formalities" relating to the relationship of a standard with the work programme, its availability in all EU languages, the transparency and inclusiveness in the course of development of the standard and the correct presence of normative references. The second step is labelled as a "quantitative verification". It requires checking that the essential requirements of EU legislation that are meant to be operationalised in a given standard are clearly and transparently identified, and that the standard does not include normative elements outside the scope of the essential requirements as identified in the Commission mandate. The third step is the one which is most relevant for the present analysis. It is called "qualitative assessment". Here the Commission (with the support of HAS consultants) has to assess whether the draft standard "sufficiently satisfies the relevant legal requirements aimed to be covered".[67] This requires, amongst others, answering whether the standard complies with the state-of-the art knowledge, whether the standard would either privilege one economic operator over others, or give choices to economic operators in such a way that the essential requirements listed in the mandate can be circumvented.

48 All in all, this checklist allows a control which is both thorough and not overly invasive. If taken seriously, it would seem to lead to a check of the content of the draft standards of such a depth and breadth that it would allow the Commission to retain sufficient knowledge and understanding of the standards (admittedly through the use of the HAS consultants) so as to avoid "opacity", while not duplicating or indeed second-guessing the work of the ESOs. The control thus carried out would not "grant unchecked epistemic authority to experts",[68] as the Commission would still remain both formally and in substance in charge of deciding whether a reference to a standard is to be published in the Official Journal.[69]

49 In the context of the AI Act, because of peculiar fundamental rights implications, the process sketched above might need to be sharpened towards the specificities of this piece of legislation. In this respect, what has been proposed in literature is a clear list of key parameters for fundamental rights risk assessment for the European Commission.[70] Research carried out on how to operationalise Article 27 of the AI Act could also prove useful in this respect.[71] Indeed, while this provision is addressed to deployers, it concerns deployers of high-risk AI systems as well as deployers "that are bodies governed by public law, or are private entities providing public services". The suggestion to use, for example, a risk index for each potentially impacted right based on a matrix combining two dimensions (likelihood of the infringement of a right and severity of that infringement)[72] could possibly also be of use for the Commission and the HES consultants when assessing the respect of draft standards with fundamental rights.

50 Finally, in light of the sensitivity of the task, more transparency in the role of the HES consultants, their mandate, their identities and their responsibility

63 See eg Oliva in this special issue.

64 European Commission, 'Verification of Conditions for the Publication of References of Harmonised Standards in the Official Journal' Ref Ares(2016)6548298 (22 November 2016).

65 Ibid, 2.

66 Ibid.

67 European Commission, Verification of conditions for the publication of references of harmonised standards in the Official Journal, (n 64) Annex I.

68 See *supra* in the Introduction on the concept of 'opacity'.

69 It has been noted that the risk exists that HES consultants could overstep their role if they interfere in the standard development process. While this opinion is entirely defensible, further empirical research would be needed in order to assess whether this risk concretely materialized. See further J Baron and P Larouche, *The European Standardisation System at a Crossroads* (n 46), 59.

70 A Mantelero 'The AI Act: a realpolitik compromise and the need to look forward' (n 14).

71 A Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template' 54 (2024) Computer Law & Security Review 106020; G Malgieri and C Santos, 'Assessing the (severity of) impacts on fundamental rights' 56 (2025) Computer Law & Security Review 106113.

72 A Mantelero, 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act' (n 71), 16.

would need to be ensured.[73] In order to avoid "capture" of HES consultants (resulting in a sort of "second-degree opacity" caused by those who were tasked to avoid it in the first place), certain independence guarantees would specifically have to be in place to ensure that they remain guarantors of the public interest in the process. Equally, the Commission would have to closely monitor the process in order to minimize the chances of "rent-seeking" behaviours, whereby HES consultants would have an incentive to "overcontrol" the draft standards in order to justify their role in the process.

D. Conclusions

51 The AI Act has entered into force in August 2024 and ESOs were tasked to develop standards for high-risk AI systems by 30 April 2025, a deadline which was not respected and extended to August 2025 and subsequently into 2026.[74] The recent Digital Omnibus on AI Proposal has further determined that certain rules governing high-risk AI systems (Chapter III, Sections 1-3) will not enter into force until the Commission has adopted a corresponding decision confirming the existence of adequate support measures for the AI Act. This decision confirms the paramount role which standards are to play in the implementation of the AI Act.[75]

52 When standards are delivered, the Commission will have the task to decide whether the draft standards will become "harmonised standards" through the publication in the Official Journal. The consequence of this publication is paramount: companies demonstrating compliance with these harmonised standards can benefit from a "presumption of conformity", which means these companies will be presumed to comply with certain elements of the AI Act unless there is evidence of non-conformity. Far from being neutral technical tools, "standards have politics",[76] they reflect "a preference for a specific logic and set of priorities",[77] they carry immense normativity. When privately developed standards acquire this peculiar public law role, it is imperative that the political choices underlying them be appropriately controlled. In specific case of the AI Act, adopted amid unprecedented political controversy,[78] and following sustained criticism on the side of both societal stakeholders[79] and academics[80] on the suitability of the use of the New Legislative Framework technique to regulate AI, the Commission's control remains a crucial juncture in the regulatory architecture.

53 The aim of this contribution has been to discuss the role of the Commission in the European standardisation process and, in particular, the scope of its control before the publication of the reference to a standard. In the aftermath of the CJEU's *James Elliott* ruling, the Commission seems to have intensified its control, a step of the process enshrined in the Standardisation Regulation. This move has attracted a substantial amount of criticism, including a possible "loss of synergies, which have historically allowed the Commission to tap into the subject matter expertise of private industry stakeholders for the development of the standards required for EU regulatory activities".[81]

54 Using a historical, teleological and systematic interpretation of the Standardisation Regulation, this contribution has demonstrated that, instead, a control of the Commission over the process and the content of draft standards is entirely allowed and in fact required by the applicable legal framework. The delays incurred in the delivery of the standards

73 See Micklitz, who argues that HAS consultants have an almost impossible task under the AI Act, requiring both expertise in law and in technology. H-W Micklitz, *The Role of Standards in Future EU Digital Policy Legislation* (n 14), 164.

74 Cynthia Kroet, 'EU standards bodies flag delays to work on AI Act' (*EuroNews*, 16 April 2025) <https://www.euronews.com/next/2025/04/16/eu-standards-bodies-flag-delays-to-work-on-ai-act> [date accessed]. This is also noted in the Commission Staff Working Document Accompanying the Digital Omnibus and Digital Omnibus on AI) COM(2025) 837 final, COM(2025) 836 final, 68.

75 Article 1(31) of the Proposal for a Regulation the European Parliament and of the Council amending Regulation (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI) SWD(2025) 836 final.

76 A Solow-Niederman, 'Can AI standards have politics?' (2024) UCLA Law Review, 231.

77 S Timmermans and S Epstein, 'A world of standards but not a standard world: Toward a sociology of standards and standardization' 36 (2010) Annual Review of Sociology, 69.

78 F Palmiotto, 'The AI Act Roller Coaster: The Evolution of Fundamental Rights Protection in the Legislative Process and the Future of the Regulation' 16 (2025) European Journal of Risk Regulation, 770.

79 C Galvagna 'Inclusive AI governance. Civil society participation in standards development' (*Ada Lovelace Institute,* 30 March 2023) <https://www.adalovelaceinstitute.org/report/inclusive-ai-governance/?utm_source=chatgpt.com> accessed March 24th 2026.

80 M Veale and F Zuiderveen Borgesius, 'Demystifying the Draft EU Artificial Intelligence Act. Analysing the good, the bad, and the unclear elements of the proposed approach 4 (2021) Computer Law Review International 97; M Ebers 'Standardizing AI: The Case of the European Commission's Proposal for an 'Artificial Intelligence Act' LA DiMatteo, C Poncibò and M Cannarsa (eds) *The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics* (Cambridge University Press, 2022), 321.

81 J Baron and P Larouche, *The European Standardisation System at a Crossroads* (n 47), 8.

and the voices raised in favour of a "pause" to the implementation of the AI Act,[82] might evoke fears that, as soon as standards are available, the Commission might be tempted to "fast-track" them to get the AI Act operational as soon as possible. These fears are further supported by the decision taken by the ESOs to skip certain stages of the standard-setting process to accelerate the delivery of harmonised standards to support the AI Act.[83] What is worse, the stages which will be compressed as a consequence of this decision are the deliberative ones, leading standard-setting power entirely in the hands of a small group of experts.[84]

55 Under these circumstances, should the Commission choose for a "rubber stamping" approach, it would contribute to the "opacity" of the legal architecture of European standardisation and, in turn, undermine its legitimacy because it would be granting indirect normative power to private standard-setting bodies. This would be all the more concerning when standards touch upon not only health and safety aspects of individuals' lives but also their fundamental rights (as is the case with the AI Act) and are linked – it can be argued – to the very upholding of the rule of law in the EU. The rushed nature of this process exacerbates these legitimacy concerns.

56 The process currently in place at the Commission, and the step it entails - if correctly carried out (through the support of the HES consultants) - would ensure a sufficient degree of control over draft standards, without the risk of "overcontrolling" on the part of the Commission. At the same time, the novelty of the fundamental right aspects of AI standards, and the delicate task of balancing fundamental rights with no specific variables or objective criteria, would seem to call for a renewed attention and possibly the need for adaptations in the process.

82 E Gkritsi, 'Europe's top CEOs ask EU to pause AI Act' (*Politico*, 4 July 2025) <https://www.politico.eu/article/top-european-ceos-plead-for-pause-in-ai-act/> last accessed April 17.

83 CEN and CENELEC, 'Update on CEN and CENELEC's Decision to Accelerate the Development of Standards for Artificial Intelligence' (*CEN-CENELEC*, 23 October 2025) <https://www.cencenelec.eu/news-events/news/2025/brief-news/2025-10-23-ai-standardization/> last accessed April 17.

84 See further on this point, M C Gamito, 'From Consensus To Exceptionality – What The EU's AI Standards Crisis Reveals About Delegated Technical Governance, (*REALaw.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 March 24th 2026

Trustworthy AI Through Standards? The Role and the Implications of Harmonised Standards for Fundamental Rights Protection in the AI Act.

by **Elvira M.R. Oliva** *

Abstract: The promotion of trustworthy Artificial Intelligence (AI), ensuring a high level of protection of health, safety, and fundamental rights, is the declared objective of the AI Act. However, since the publication of the proposal by the EU Commission and throughout the entire legislative procedure, the indeterminacy of several key provisions has fuelled the scholarly debate. In this context, the presumption of conformity, enshrined in Article 40 of the AI Act, applicable to high-risk and general-purposes AI models complying with harmonised technical standards (HTS), assumes a pivotal function for providers. While the recourse to harmonised standards is not new in EU law, scholars have emphasized numerous controversial aspects of the process of entrusting the determination of harmonised standards to private bodies, i.e. European Standards Organizations (ESOs). The contribution focuses on the role of harmonised standards for fundamental rights protection, scrutinising their relevance within the broader AI Act architecture specifically for high-risk AI systems. Firstly, it examines the relationship between the risk approach to fundamental rights and harmonised standards. Secondly, it explores the adequacy and the implications of the recourse to HTS in the fundamental rights realm, in light of the delegation doctrine. Ultimately, it argues that HTS are structurally ill-suited to ensure effective fundamental rights protection from AI risks.

Keywords: Artificial Intelligence, fundamental rights, AI Act, risk regulation, New Legislative Framework.

Recommended citation: Elvira M.R. Oliva, Trustworthy AI Through Standards? The Role and the Implications of Harmonised Standards for Fundamental Rights Protection in the AI Act.I, 17 (2026) JIPITEC 61 para 1.

A. Introduction

1 The summer[1] of Artificial Intelligence (AI) has reignited the debate on the relationship between law and technology, and on whether the law merely reacts to or actively shapes socio-technical changes, with a consequent confrontation between proponents of tech-exceptionalism and defenders of the *Law of Horses.*[2] On this path, recently, various jurisdictions have entered the race to regulate AI,

* PhD Candidate in EU Law, University of Bologna.

1 Youjung Shin, 'The Spring of Artificial Intelligence in its global winter' (2019) 41 IEEE Annals of the History of Computing 71.

2 The debate has emerged firstly regarding the intricacies of the relationship between law and technology and recently moved to discussing the appropriateness of specific legal initiatives to regulate new technologies. These discussions are split between the literature supporting the risk of a new *Law of Horses* and that reaffirming the necessity to legally tackle the challenges of new technologies, even re-imagining of traditional law categories. See *inter alia*: Natalino Irti, Emanuele Severino *Dialogo su diritto e tecnica* (Laterza 2001); Frank H. Easterbrook, 'Cyberspace and the Law of the Horse" (1996) 1996 University of Chicago Legal Forum 207; Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113/2 Harvard Law Review 501; Roger Brownsword, 'Law, innovation and technology: fast forward to 2021' (2021) 13/1 Law, Innovation & Technology 1; Ryan Calo, 'Robotics and the Lessons of Cyberlaw' 103 California Law Review 513.

proposing different legal approaches.[3] Within this context, the European Union (EU) has opted for an *ad hoc* legislative act aimed at fostering a human-centric ecosystem of trust aligned with EU values and principles, while promoting innovation.[4]

2 The EU Regulation (AI Act)[5] lays down harmonised rules for the development, placement on the market, and use of AI systems. From its first recital,[6] the Regulation sets out its dual objective: to ensure secure and trustworthy AI protecting fundamental rights, and to facilitate the effective functioning of the internal market for AI uptake. It thus attempts to combine two foundational pillars of EU law, namely product safety harmonisation and fundamental rights protection,[7] through a risk-based approach:[8] the intensity of the regulatory burden depends on the likelihood and significance of risks posed by the AI system to safety, health, and fundamental rights. Along these lines, the AI Act introduces a layered risk pyramid with corresponding legal regimes: a ban for systems posing unacceptable risks; *ex ante* requirements and *ex post* monitoring obligations for high-risk systems, which constitute the core of the Regulation, minimal duties for the remaining low-risk systems,[9] and a specific regime for most advanced general-purposes AI models.[10] The risk-based approach is not novel in EU law.[11] Even with different nuances, the most relevant EU legislative initiatives in the digital domain have embraced it to foster innovation while ensuring the protection of fundamental rights. This is the case for the General Data Protection Regulation (GDPR)[12] and the Digital Services Act (DSA).[13]

3 The AI Act follows this route by relying on the most common risk-based regulatory instruments: precautionary tools, risk management and mitigation duties, and post-market measures.[14] Within this regulatory architecture, the concept of risk acquires both a foundational and functional value, serving as an anchor for the framework and guiding the allocation of legal obligations. Notably, the key notion of trustworthiness is defined in terms of the acceptability of risk and is tied to compliance obligations for high-risk AI systems.[15] The Regulation presumes that AI- related risks can be quantified and measured, implying a binary and static relationship between the AI system, as a source of harm, and its effects on three dimensions:

3 Nathalie A. Smuha, 'From a 'Race to AI' to a 'Race to AI Regulation' - Regulatory Competition for Artificial Intelligence' (2021) 13 Law, Innovation & Technology 57.

4 European Commission, On Artificial Intelligence- A European approach to excellence and trust COM (2020) 65 final.

5 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 (AI Act), OJ L 12.07.2024.

6 Recital 1 states that the purpose of the Regulation is "to improve the functioning of the internal market, promoting the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union, including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation (..)".

7 Marco Almada, 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 85.

8 Recital 26 of the AI Act.

9 Art. 50 of the AI Act.

10 Chapter V of the AI act.

11 Examples come from various sectors: food safety, environmental and financial regulation. See inter alia: Springer, Marian Garcia Martinez, Paul Verbruggen, Andrew Fearne, 'A. Risk-based approaches to food safety regulation: what role for co-regulation?' (2013) 16/9 Journal of Risk Research, 16(9) 1101; Katalin Mérő, 'The ascent and descent of banks' risk-based capital regulation' (2021) 22 Journal of Bank Regulation 308.

12 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR), OJ L119/1. On the notion of risk in GDPR see: Robert Gellert, 'Understanding the notion of risk in the General Data Protection Regulation' (2018) 34 Computer Law & Security Review 279.

13 Art. 34 of DSA defines the methodology and timing to perform risk assessment, specifically considering any actual or foreseeable negative effects for the exercise of fundamental rights, in particular to human dignity, to respect for private and family life, to the protection of personal data, to freedom of expression and information, including the freedom and pluralism of the media, to non-discrimination, to respect for the rights of the child and to a high-level of consumer protection, as enshrined in the Charter of fundamental rights. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act, DSA), OJ L 277.

14 Margot Kaminski, 'Regulating the risks of AI' (2023) 103 Boston University Law Review 1347.

15 Recital 123: "In order to ensure a high level of trustworthiness of high-risk AI systems, those systems should be subject to a conformity assessment prior to their placing on the market or putting into service". See: Johann Laux, Sandra Wachter, Brent Mittelstadt, 'Trustworthy artificial intelligence and the European Union AI act: On the conflation of trustworthiness and acceptability of risk' (2024) 18/1 Regulation & Governance 3.

health, safety, and fundamental rights. Accordingly, the classification of an AI system in the diverse risk categories depends on its impact on health and safety, as in the typical product safety legislation[16] with, in addition, fundamental rights. In this context, fundamental rights protection is not only a legal parameter but also a rationale for pre-categorising the AI systems use cases[17] and, determining the applicable legal regime. Unlike other EU's digital regulation, such as the GDPR and the DSA, tailored to the protection of specific rights, respectively the right to data protection[18] and freedom of expression and of information,[19] the AI Act aims to safeguard all fundamental rights at stake, reflecting the diverse AI use cases it encompasses.

4 This comprehensive ambition is challenged by a continuously evolving material scope. During the legislative procedure, the release of ChatGPT[20] has prompted the introduction of an additional category to address the systemic risks[21] stemming from the most powerful and promising general-purpose AI systems. To bridge future potential gaps between the rapidity of technological development and the slower pace of legislative update,[22] the Regulation has been designed to ensure both legal certainty and flexibility to face emerging AI models and use cases.[23] To this aim, the AI Act relies on soft law[24] and hybrid regulatory tools, such as Harmonised Technical Standards (HTS),[25] particularly relevant in high-risk AI systems where potential threats to fundamental rights have already emerged or are supposed to occur in the short term.[26] In these cases, the Regulation stipulates a continuous, lifecycle-wide risk management process aimed at preventing or minimising the relevant risks to health, safety and fundamental rights.[27] Specifically, it sets out requirements to be ensured by design, together with procedural obligations in terms of registration and documentation before the placement into market/use of the system. The technical translation of the *ex ante* requirements[28] is delegated to European Standardisation Organisations (ESOs) through HTS, adherence to which grants a presumption of conformity, as enshrined in Article 40. In particular, the HTS are expected to define detailed specifications for the management and mitigation of risks to health, safety, and fundamental rights.

5 While the recourse to HTS as a driver for internal market harmonisation is well-established and its legal challenges have been relevantly investigated,[29] its use in the realm of fundamental rights is a novelty, which revamps the traditional legal concerns raised by HTS with new nuances. In particular, the essence

16 In the Product Safety Regulation a safe product is defined as: "any product which, under normal or reasonably foreseeable conditions of use, including the actual duration of use, does not present any risk or only the minimum risks compatible with the product's use, considered acceptable and consistent with a high level of protection of the health and safety of consumers" according to art. 3 (2), Regulation (EU) 2023/988 of the European Parliament and of the Council 10 May 2023 on general product safety, amending Regulation (EU) No 1025/2012 of the European Parliament and of the Council and Directive (EU) 2020/1828 of the European Parliament and the Council, and repealing Directive 2001/95/EC of the European Parliament and of the Council and Council Directive 87/357/EEC, OJ L 135.

17 The categories of risk are defined in the Regulation, following a top-down approach. For a comparison with the bottom-up approach in GDPR and the mixed approach in DSA see: Giovanni De Gregorio, Pietro Dunn, 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age' (2022) 59 Common Market Law Review 473.

18 Recital 1 of the GDPR.

19 Recital 3 of the DSA.

20 The release of ChatGPT on 30th November 2022 disrupted the discussion on the AI Act, which initially did not cover foundational models and general-purpose AI systems in its material scope. Consequently the co-legislators modified the text including general-purposes AI systems in Art. 3 (63): "AI systems based on a model trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications".

21 Art. 3 (65) of the AI Act.

22 Gary E. Marchant, Braden E. Allenby, Joseph R. Herkert (eds.), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight* (Springer 2011).

23 Stefan Larsson, Jockum Hildén, Kasia Söderlund, 'Implications of Regulating a Moving Target: Between Fixity and Flexibility in the EU AI Act' <https://ssrn.com/abstract=5211101> accessed 18.04.2025.

24 Art. 96 of the AI Act on the guidelines to be issued by EU Commission.

25 Art. 3 (27) of the AI Act.

26 The list of high-risk systems refers both to systems integrated as part of products already in the scope of harmonised legislation (ANNEX I) and to stand-alone systems (ANNEX III) of the AI Act.

27 Art. 9 mandates the establishment of a risk management system to be implemented, documented and maintained. It is based on processes and testing procedures. See Jonas Schuett, 'Risk Management in the Artificial Intelligence Act' (2024) 15 European Journal of Risk Regulation 367.

28 Chapter III, Section 2 of the AI Act.

29 Harm Schepel, *The Constitution of Private Governance: Product Standards in the Regulation of Integrating Markets* (Hart 2005); Mariolina Eliantonio, Caroline Cauffman, 'The Legitimacy of Standardisation as a Regulatory Technique in the EU – A Cross-disciplinary and Multi-level Analysis: An Introduction' in Mariolina Eliantonio, Caroline Cauffman (eds), *The Legitimacy of Standardisation as a Regulatory Technique* (Edward Elgar Publishing 2020).

of fundamental rights[30] requires context-specific assessments to verify if its exercise is impaired by an interference without legitimate reasons;[31] thus, it escapes from the static and quantitative logic[32] of the traditional product standardisation procedure. High-risk AI systems may affect a plurality of fundamental rights, thereby giving rise to complex normative questions, which necessitate a balancing of rights and interests at stake.[33] In this line, the entrusting to ESOs of such delicate task may challenge the boundaries of the delegation doctrine.

6 Against the backdrop of these introductory remarks, the contribution asks whether Harmonised Standards (HTS), as envisioned in the EU AI Act, are suitable tools for managing risks to fundamental rights. To answer this question, it proceeds as follows: section B examines the role of HTS within the broader architecture of the AI Regulation, focusing on their intended function in managing high-risk to fundamental rights; section C critically assesses the main legal challenges stemming from HTS when dealing with fundamental rights. The challenges will be examined through the delegation doctrine lens and will underscore the limits, and the prospects of the potential compensatory mechanisms envisaged in the AI Act, namely common specifications and the Fundamental Rights Impact Assessment (FRIA), drawing on Court of Justice of the European Union (CJEU) case law and legal doctrine. The conclusions summarize the key findings and propose a potential pathway.

B. Embedding Fundamental Rights Dimension Into Technical Norms? The Role of Harmonised Standards in the AI Act

7 The AI Act reliance on HTS follows a well-established path of EU Legislation, started in the mid-80s, with the New Approach,[34] and refined through the New Legislative Framework (NLF)[35] aimed at harmonising the EU internal market products and enhancing legislative efficiency, establishing a common framework of general principles to approximate products' legislation. Normatively, the NLF complements the traditional top-down legislative approach with alternative regulatory and non-regulatory tools,[36] precisely self- and co-regulation,[37] to govern complex societal and

30 The concept of *essence* has been set out in the Article 52(1) of Fundamental Rights of the European Union, as a condition to be fulfilled to justify any limitation of a fundamental right. According to the CJEU case law, the essence of fundamental rights refers to its "very substance." Broadly, it implies that any limitation to one of the fundamental rights enshrined in the Charter which does not respect its essence should be considered unlawful, without regard of the possible general interest pursued by the limitation. In this vein, it requires the consideration of the normative elements of each fundamental right at stake together with the characteristics of the case. On the issue see *inter alia*: Koen Lenaerts, 'Limits on Limitations: The Essence of Fundamental Rights in the EU' (2019) 20 German Law Journal 779; Maja Brkan, 'The Concept of Essence of Fundamental Rights in the EU Legal Order: Peeling the Onion to its Core' (2018) 14/2 European Constitutional Law 339; Tuomas Ojanen, 'Making the Essence of Fundamental Rights Real: The Court of Justice of the European Union Clarifies the Structure of Fundamental Rights under the Charter: ECJ 6 October 2015, Case C-362/14, Maximillian Schrems v Data Protection Commissioner' (2016) 12 European Constitutional Law Review 318.

31 The protection of the *essence* of a fundamental right requires an evaluation which differs from the proportionality test. More precisely "proportionality begins where essence stops": see Takis Tridimas and Giulia Gentile, 'The Essence of Rights: An Unreliable Boundary?' (2019) 20 German Law Journal 794, 803.

32 On the attempt to quantitatively measure fundamental rights with a proportionality lens see: Giovanni Sartor, 'The Logic of Proportionality: Reasoning with Non-Numerical Magnitudes' (2013) 14/8 German Law Journal 1419.

33 In this context, the balancing exercise should be considered as the *ad hoc* activity to solve potential conflicts arising when at least one fundamental right enshrined in the Charter of Fundamental Rights is competing either with a public interest or with another fundamental right. See *inter alia*: Matthias Klatt and Moritz Meister, *The Constitutional Structure of Proportionality* (Oxford University Press 2012).

34 Council Resolution 85/C 136/01 of 7 May 1985 on a new approach to technical harmonisation and standards. OJ C 136, 4.6.1985, p. 1–9.

35 Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products; Decision 768/2008 on a common framework for the marketing of products, which includes reference provisions to incorporate in product legislation revisions; Regulation (EU) 2019/1020 on market surveillance and compliance of product, OJ L 169, 25.6.2019, p. 1–44.

36 Better Regulation Toolbox, July 2023 ed. <https://commission.europa.eu/document/download/9c8d2189-8abd-4f29-84e9-abc843cc68e0_en?filename=BR%20toolbox%20-%20Jul%202023%20-%20FINAL.pdf> accessed 12.11.2024.

37 "Co-regulation means the mechanism whereby a community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognised in the field (such as economic operators, the social partners, non-governmental organisations, or associations). Self-regulation is defined as the possibility for economic operators, the social partners, non-governmental organisations, or associations to adopt amongst themselves and for themselves common guidelines at the European level (particularly codes of practice or sectoral agreements)." Interinstitutional agreement on better law-making, OJ C 321, 31.12.2003.

technological changes, as framed within the Better Regulation agenda.[38] The consequent shift from the traditional "command and control" model[39] to more decentralised governance forms[40] has opened the regulatory space to private and non-institutional actors, such as European Standardisation Organisations (ESOs).[41]

8 Broadly, the NLF seeks to preserve the binding nature of legislation while allowing for flexible implementation, thereby accelerating market harmonisation and boosting innovation.[42] In this respect, it aligns with the same challenges prompting the recourse to risk regulation, relying on technocratic approaches to enhance regulatory efficiency, objectivity, and fairness for businesses.[43] Accordingly, in principle, the integration of a risk-based approach with the implementation toolkit provided by NLF seems particularly well-suited to regulate a highly technical and constantly evolving domain like AI, especially from an internal market perspective.[44]

9 The AI Act explicitly embraces the NLF[45] and refers to its catalogue of self and co-regulation tools for implementation,[46] considering HTS as a key compliance mechanism[47] for managing high risks to health, safety, and fundamental rights. Specifically, the adherence to HTS enables providers to conduct a conformity assessment based on internal controls, without involving external actors.[48] Alternatively, the providers may opt for third-party assessments, which are more costly and resource demanding. It is therefore reasonable to expect that providers of high-risk systems will prefer HTS to manage risks to fundamental rights, leveraging the simplified compliance mechanism. As confirmed by CJEU case law, HTS are *de jure* voluntary, but *de facto* mandatory.[49] This quasi-obligatory nature underscores their significance within the AI Act's compliance architecture, especially considering their novel function in operationalising management of risks to fundamental rights.[50] However, despite this heightened importance, an analysis of Article 40 and the Commission's Standardisation Request[51] reveals that AI HTS are expected to follow the traditional path of product technical standardisation, without specific adaptations to the fundamental rights' domain.

38 Starting with Better Regulation for Growth and Jobs in the European Union, COM (2005) 97 final, Brussels, 16.3.2005.

39 Robert Baldwin, Martin Cave, Martin Lodge (eds) *Understanding Regulation – Theory, Strategy and Practice* (Oxford, 1999).

40 Julia Black, 'Decentring Regulation: Understanding the Role of Regulation and Self-regulation in a 'Post-regulatory' World' (2001) 54/1 Current Legal Problems 121.

41 CEN, CENELEC, ETSI, in Annex I Regulation (EU) 1025/2012 Regulation 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 (Standardisation Regulation) OJ L 316.

42 Better Regulation Toolbox, July 2023 ed. <https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox/better-regulation-toolbox_en> accessed 04.05.2025.

43 Bridget Hutter, 'A risk regulation perspective on regulatory excellence' in Cary Coglianese (ed.), *Achieving Regulatory Excellence* (Brookings Institution Press, 2017) 101.

44 The legal basis of the AI Act is the Article 114 TFEU used "to prevent the occurrence of these obstacles resulting from diverging national laws and approaches how to address the legal uncertainties and gaps in the existing legal frameworks applicable to AI (..) The new initiative will aim to address that problem by proposing harmonised technical standards for the implementation of common requirements applicable to the design and development of certain AI systems before they are placed on the market (...)in addition, considering that this Regulation contains certain specific rules, unrelated to the functioning of the internal market, restricting the use of AI systems for 'real-time' remote biometric identification by the law enforcement authorities of the Member States, which necessarily limits the processing of biometric data by those authorities, it is appropriate to base this Regulation, in as far as those specific rules are concerned, on Article 16 of the Treaty." European Commission, Impact Assessment accompanying the Proposal for a Regulation laying down harmonised rules on Artificial Intelligence, SWD (2021) 84 final, p. 31.

45 The reference to New Legislative Framework appears both in reference to general structure of AI Act, see Recital 9, and related to specific provisions on high-risk AI systems, see Recitals 46, 64, 83, 84, 87, 124.

46 Art.56 introduces the Code of practices for providers of general-purpose AI models, drawn up by providers, national authorities with other stakeholders supporting the process. Art. 95 refers to codes of conduct to foster voluntary application of requirements established for high-risk cases for minimal risk systems.

47 Recital 121 of the AI Act.

48 Art. 43 of the AI Act.

49 Case C-171/11 *Fra.Bo SpA v DVGW* (2012) EU:C:2012:453, paras 27 to 32.

50 Josep Soler Garrido, Sarah De Nigris, Elias Bassani, Ignacio Sanchez, Tatjana Evas, André Antoine-Alexandre, Thierry Boulangé, 'Harmonised Standards for the European AI Act' (2024) JRC139430.

51 European Commission Implementing Decision C (2023) 3215 final. The decision has been repealed by the European Implementing Decision C (2025) 3871 final which adjusts the timeline while maintain the content of the Request from Commission to CEN and CENELEC.

10 Although Article 40 underwent amendments during the legislative procedure, its core structure remains aligned with the traditional HTS framework, as in the original Commission proposal.[52] Firstly, the final version of the Article expands its material scope to the general-purpose AI models,[53] in addition to high-risk systems as initially foreseen, consistently with the inclusion of such systems in the scope of the Regulation. Secondly, as proposed both in Council and EU Parliament amendments,[54] a reference to appropriate stakeholders' participation has been added, without, however, introducing new binding requirements for the AI standardisation process beyond the provisions already established in Regulation (EU) 1025/2012.[55] While an *ad hoc* AI Task Group on inclusiveness has been launched to raise awareness and bring new stakeholders to the discussions within the ESOs, the effort remains within the spirit and the letter of the existing Regulation,[56] thus not formally enhance participation of the new actors.[57] Importantly, the final version of Article 40(3) emphasises that HTS must be consistent with Union values, fundamental rights, and interests, also related to international cooperation. Crucially, HTS are not merely expected to consider EU values, but they must operationalise management and mitigation of risk to fundamental rights, alongside health and safety.

11 This expectation is clearer in the Request[58] to CEN and CENELEC,[59] issued by Commission in May 2023, during the AI Act legislative procedure. The two ESOs have been tasked with drafting the first set of HTS, which should reflect the generally acknowledged state of the art to prevent and minimise risks to health, safety, and fundamental rights, as guaranteed in the Charter of Fundamental Rights and in relevant EU law, to cover the requirements established in the Regulation. Nevertheless, in the case of fundamental rights, the operationalisation of requirements not only deals with technical specifications, but it also implies guidance on complex rights-related normative issues.[60] A non-exhaustive but immediate sample is offered by the data set requirements: the AI Act mandates the detection, prevention, and mitigation of potential biases of data that could have an adverse impact on fundamental rights.[61] In particular, the quality and the representativeness of datasets used for AI systems training and validation could affect rights to privacy as well as non-discrimination, and, depending on the context of use, further fundamental rights and interests[62] In this line, ESOs are tasked with providing orientation to navigate the complex balancing of fundamental rights required when two or more rights and interests are at stake. It could be contended that HTS merely perform a procedural operationalization of rights, standardizing risk management methodologies. However, when an HTS establishes the acceptable threshold for risk to fundamental rights, it is not

52 In the Commission proposal, Article 40: "High-risk AI systems which are in conformity with harmonised standards or parts thereof the references of which have been published in the Official Journal of the European Union shall be presumed to be in conformity with the requirements set out in Chapter 2 of this Title, to the extent those standards cover those requirements." Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. COM (2021) 206 final.

53 See n 19.

54 In the Council's proposal: enhance multistakeholder governance, representative of all relevant European stakeholders (e.g. industry, SMEs, civil society, researchers) Council, General Approach 14336/22 25.11.2022; in the Parliament's amendment: a balanced representation of interests and effective participation of all relevant stakeholders in accordance with Articles 5, 6, and 7 of the Standardisation Regulation. European Parliament, Negotiation Position, P9_TA (2023)0236 14.06.2023.

55 See n 40.

56 Art. 3 of the Standardisation Regulation.

57 Art. 5 of the Standardisation Regulation, which has been amended in 2023 introducing limited changes in the standardisation process, specifically to reinforce national organizations' role and to require the publication of the deliverables plans from the ESOs. Despite the numerous concerns highlighted by doctrine and related to CJEU's case law, the legislative changes have not yet solved either transparency or accountability shortcomings, with no mandatory participation for enhancing civil society representativeness. See: Annalisa Volpato, Mariolina Eliantonio, 'The participation of civil society in ETSI from the perspective of throughput legitimacy' (2024) 37/5 Innovation: The European Journal of Social Science Research 1375.

58 See Annex II, point 2 of the Implementing decision (n 51)

59 On ETSI's exclusion see: Marta Cantero Gamito, 'The Role of ETSI in the EU's Regulation and Governance of Artificial Intelligence' (2024) Innovation: The European Journal of Social Science Research, available at SSRN <http://dx.doi.org/10.2139/ssrn.4770324> accessed 22.04.2025.

60 Johann Laux, Sandra Wachter and Brent Mittelstadt, 'Three Pathways for Standardisation and Ethical Disclosure by Default under the European Union Artificial Intelligence Act' (2024) 53 Computer Law & Security Review.

61 Art. 10 of the AI Act.

62 See *inter alia*: Raphaele Xenidis, 'When Computers Say No: Towards a Legal Response to Algorithmic Discrimination in Europe' in Bartosk Brożek, Przemyslaw Palka, Olga Kanevskaia (eds), *Research Handbook on Law and Technology* (Edward Elgar Publishing 2024), 222; Keith Sonderling, Aram Gavoor, 'A New Approach to Measuring AI Bias in Human Resources Functions: Model Risk Management'(2023) 54/4 Seton Hall Law Review 965; Uwe Peters, 'Algorithmic Political Bias in Artificial Intelligence Systems' (2022) 35/2 Philosophy & Technology.

merely performing procedural task, it is engaging in a substantive balancing of rights, which goes beyond a pure technical translation of legislative requirements

12 Finally, it should be noted that during the AI Act legislative process, the Commission has released a new EU Standardisation Strategy,[63] which recognises the essential role of standards for the internal market and EU competitiveness, particularly at the international level, while highlighting its participation and transparency shortcomings. Interestingly, the new Strategy acknowledges that standards deal not only with technical components but also incorporate and promote EU core values and interests. As a matter of fact, with the new Strategy, the Commission confirms that technicalities cannot be separated from normative values,[64] which is particularly evident in legislative acts like the AI Act, where HTS are expected to define methods to ensure a proper fundamental rights protection from current and potential harms posed by high-risk AI systems, in addition to their traditional function for the internal market harmonisation.

13 This section has highlighted the pivotal role assigned by the AI Act to HTS in managing and mitigating risks to fundamental rights to ensure conformity of high-risk systems, recently confirmed by the Commission proposal for a postponement of high-risk implementation timeline linked to the availability of HTS.[65] While embedding the rights-based dimension into the standardisation process constitutes a novelty, it remains situated within the traditional product standardisation framework. The analysis of Article 40, read in conjunction with the Standardisation Request, suggests that AI HTS for fundamental rights would not depart from the existing regimes established for traditional product-related HTS.

63 An EU Strategy on Standardisation Setting global standards in support of a resilient, green, and digital EU single market, COM (2022) 31 final, specifically on the promotion of EU values see p.4.

64 On the difficulties and implications to separate 'technical' from 'value-laden' considerations in HTS see Schepel (n 27), 255.

65 Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) 2024/1689 and (EU) 2018/1139 as regards the simplification of the implementation of harmonised rules on artificial intelligence (Digital Omnibus on AI), COM(2025) 836 final.

C. Legal Challenges of Harmonised Standards in the Management of Risks to Fundamental Rights

14 The reliance on HTS as a tool to operationalise fundamental rights protection in the management of risks posed by high-risk AI systems raises acute legal concerns, stemming from value-laden and normative judgments required, which ought to be assessed through the lens of the EU's delegation doctrine.

15 Since the landmark *Meroni* ruling,[66] the CJEU has recognised that executive powers may be delegated by the entitled institutions to private third parties only under specific and strict conditions, within the limits settled in the Treaties.[67] Particularly, it has been established the requirements for both a clear executive mandate, according to objective and precise criteria, and a strict oversight by the delegating institution, to prevent the exercise of a discretionary power[68] and the consequent shift of responsibilities towards delegated subjects, which would undermine the principle of institutional balance.[69] The CJEU has reaffirmed this reasoning, with a non-formalistic approach, in the *ESMA* case,[70] allowing a broader delegation to public Union bodies, offices or agencies, provided that judicial review mechanisms are in place,[71] the delegated entities possess the necessary technical expertise,[72] and a detailed delineation of the powers is well established.[73] The possibility of entrusting[74] power

66 Case C-10/56 *Meroni v High Authority of the European Coal and Steel Community* (1958), EU:C:1958:7.

67 ibid, para 173.

68 For an analysis of the relevance and the implications of the definition of discretionary power in the case law see Joana Mendes, 'Law, Public Interest and Interpretation: Prolegomena of a Normative Framework on Administrative Discretion in the EU' (2014) 519 Yale Law & Economics Research Paper.

69 Maria Patrin 'Meroni behind the scenes: uncovering the actors and context of a landmark judgement' (2021) 6/1 European Papers 539.

70 Case C- 270/12 *UK v European Parliament and Council of the European Union* (2014) EU:C:2014:18.

71 ibid, para 80.

72 ibid, paras 82 and 105.

73 ibid, para 51.

74 It should be noted that the Court relates to an entrusting process, avoiding the word «delegation», see Case C-613/14 *James Elliott Construction Limited v. Irish Asphalt Limited* (2016) EU:C:2016:821, para 43. Differently, the Advocate General expressly refers to a legislative «controlled delegation» to private organisations, see Case C-613/14 *James Elliott Construction Limited v. Irish Asphalt Limited* (2016) EU:C:2016:63, Opinion of A.G. Bordona, para. 55.

to private third parties has been expanded with the seminal *James Elliott* case,[75] a preliminary ruling where the Court has established its interpretive jurisdiction on HTS, stating that, once referenced in the Official Journal by the Commission, HTS form part of EU law with legal effects, since compliance with such standards grants a presumption of conformity with essential requirements of the legislative act originating the delegation.[76] Within this framework, it could be inferred that ESOs must operate under a clear mandate and the standardisation process must be subject to a strict control by the Commission to avoid an unlawful transfer of power, as prohibited by the *Meroni* doctrine, in addition to a judicial reviewability and the professional expertise, as established in *ESMA* case, here recalled by analogy. Against this backdrop, the next paragraphs will examine whether the use of HTS for management of AI risks to fundamental rights comply with these requirements.

16 In the context of the AI Act, the EU Commission Standardisation Request issued pursuant Article 40 can be interpreted as the act of entrustment. Nonetheless, the compliance with the delegation doctrine's requirement for a clear and precise mandate is highly contestable, particularly with respect to fundamental rights, given the vague wording employed in both the Standardisation Request and the Regulation. Indeed, the AI Act broadly and generically refers to fundamental rights,[77] but fails to clarify criteria and procedures to assess and mitigate risk to fundamental rights, thus a clear guidance to be operationalised by HTS is lacking.[78] The only identifiable criteria emerge in relation to the future possibility to amend the Annex on high-risk AI systems list,[79] recalling the approach followed by Commission in its proposal.[80] Moreover, apart from the recitals,[81] the Regulation does not define which specific rights are at risk and how they should be protected in the diverse high-risk scenarios.

17 Article 40(3) calls for consistency of HTS with Union values and fundamental rights, as a legal parameter, without detailing the requirements to technically translate fundamental rights protection. Similarly, the Standardisation Request reiterates the importance of compliance with fundamental rights and EU Charter values, again, with no further details, leaving the mandate unclear.[82] This vagueness is critical not only from a delegation perspective, but even under NLF, whose legislative framework prescribes that legislative provisions must be worded with sufficient clarity and precision to establish legally binding obligations,[83] to ensure that the technical specifications developed by standardisation bodies remain within the boundaries of the legislative mandate and do not result in the exercise of normative and political discretion by private actors.[84] Importantly, the determination of methods for establishing thresholds of acceptable risk to fundamental rights[85] is not merely a technical or procedural exercise but a normative task that inherently involves value-based judgment, which requires a clearer mandate to comply with *Meroni* doctrine.

18 It may be argued that the Standardisation Request and the Regulation's vagueness could be mitigated by a rigorous control mechanism implemented by the Commission during the standardization process

75 ibid.

76 ibid, para 40.

77 The reference to "fundamental rights" occurs 103 times: 56 in the Recitals, 47 in the Articles.

78 Alessandro Mantelero 'The AI Act: a realpolitik compromise and the need to look forward in Digital Constitutionalism' (2025) Nomos 311.

79 Art. 7 (2) of the AI Act.

80 "These criteria include: a) the extent to which an AI system has been used or is about to be used; b) the extent to which an AI system has caused any of the harms referred to above or has given rise to significant concerns around their materialization; c) the extent of the adverse impact of the harm; d) the potential of the AI system to scale and adversely impact a plurality of persons or entire groups of persons; e) the possibility that an AI system may generate more than one of the harms referred to above; f) the extent to which potentially adversely impacted persons are dependent on the outcome produced by an AI system, for instance their ability to opt-out of the use of such an AI system; g) the extent to which potentially adversely impacted persons are in a vulnerable position vis-à-vis the user of an AI system; h) the extent to which the outcome produced by an AI system is reversible; i) the availability and effectiveness of legal remedies; j) the extent to which existing Union legislation is able to prevent or substantially minimize the risks potentially produced by an AI system". Impact Assessment (n 43), p.50.

81 See Recital 48-62 of the AI Act. On the limits of recitals: Maarten Den Heijer, Teun Van Os Van Den Abeelen and Antanina Maslyka, 'On the Use and Misuse of Recitals in European Union Law' (2019) 31 Amsterdam Law School Research Paper.

82 While the standardisation process is still in progress, from the public documentation it can be derived that the operationalisation of fundamental rights dimension could be absorbed in the main HTS related to AI Risk Management and Trustworthiness Framework, instead of treated in a specific item, as originally foreseen.

83 Recital 11 Decision 768/2008 (n 34).

84 European Commission, Vademecum on European Standardisation – Part I, SWD (2015) 205, 8-9.

85 See: AI Risk Management, prEN 18228, https://standards.cencenelec.eu/dyn/www/f?p=205:110:0::::FSP_PROJECT,FSP_LANG_ID:79438,25&cs=1CB88DD3F349909A6F65743B3FBFF0992 accessed 19.07.2025.

and before the publication of the references in the Official Journal, which would involve conducting the compliance assessment.[86] It is worth noting that the Request allows the Commission to monitor project plans and assess the deliverables for consistency with fundamental rights and data protection laws, accounting for both common horizontal risks and potentially vertically specific standards related to intended purposes and/or context uses of AI high-risk systems.[87] However, while formally this complies with the requirement of the delegation doctrine, the substantial effectiveness of the oversight could be limited by the lack of the technical capacity to navigate complex AI standards.[88]

19 Under these circumstances, the concerns of tasking ESOs with guidance on fundamental rights are further amplified given that high-risk AI systems engage diverse fundamental rights and interests, intersecting or even conflicting,[89] both at individual and societal levels.[90] When diverse fundamental rights are at stake, the establishment of compliance pathways implies indications on a delicate balancing exercise governed by the principle of proportionality. As enshrined in the EU Charter of Fundamental Rights[91] and constantly emphasised in the CJEU case law,[92] any potential limitations on fundamental rights require a well-defined scope of the measures providing for an interference and the conditions of their applicability. Specifically, in the case of the AI systems, the balancing would need to account not only for individual fundamental rights but also for broader public interests[93] and economic freedom of providers to conduct business and their legitimate expectations to market access when adhering to HTS.[94]

20 Drawing a parallel with data protection law, where such balancing is established, may serve to underscore the flaw in the AI Act. Under GDPR, where a data processing is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall perform a data protection impact assessment (DPIA):[95] an *ex ante* evaluation containing, *inter alia,* an analysis of the necessity and proportionality of the operations, including the legitimate interest pursued and the risks to rights for data subjects, considering the scope, the context and the purpose of the activity, together with mitigation measures. Significantly, the DPIA is grounded in the principle of accountability,[96] establishing the discretion of the regulated subjects within a clear legal framework. In this context, an operational guidance on balancing methodologies is offered by *ad hoc* Guidelines adopted by Data Protection Authorities, which provide interpretative direction within a clearly define mandate.[97] Conversely, under the AI Act, the task of defining balancing methodology[98] is instead entrusted to the ESOs, private third parties, through HTS, which, once referenced in the Official Journal, grant the presumption of conformity for management of risks to fundamental rights. This divergence is relevant when assessing the procedural rather than the substantive nature of HTS. Far from serving as guidance, HTS are expected to serve as a compliance tool through which high-risk AI systems demonstrate conformity with the AI Act, thus entering into the EU market.[99]

86 Vademecum (n 84), p. 26-27.

87 Annex II, point 1 of the Implementing Decision. It should be noted that, in its latest Request, the Commission requests a report from ESOs every three months, instead of six months established in the previous one. (n 51).

88 Megi Medzmariashvili, 'Delegation of Rulemaking Power to European Standards Organizations: Reconsidered' (2017) 44 Legal Issues of Economic Integration 353, 361.

89 See Impact Assessment accompanying the proposal of Regulation, SWD (2021) 84 final, point 5.5.

90 Confirmed in the scope of AI Risk Management HTS (n 85).

91 Art. 52 (1) of the Charter of Fundamental Rights.

92 C-817/19 *Ligue de droits* (2022) EU:C:2022:65, Opinion of A.G Pitruzzella, paras 85-88 and cited case-law.

93 Article 5 of the Convention 108+ ; Case C-470/21 *La Quadrature du Net* (2024) EU:C:2024:370, para 130.

94 The European Court of Human Rights has repeatedly intervened on the issue, see *inter alia: Roman Zakharov, v Russia* App no. 47143/06 (ECHR, 4 December 2015); *Malone v UK* Application App no. 8691/79 (ECHR, 2 August 1984).

95 Art. 35 of GDPR.

96 Art. 5(2) of GDPR. See *inter alia*: Tuulia, Karjalainen, 'All talk, no action? The effect of GDPR Accountability Principle on the EU Data Protection paradigm' (2022) 8(1) European Data Protection Law Review, 19.

97 See Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP 248 rev.01, adopted 4 April 2017 by Article 29 Working Party Data Protection.

98 See the description of the HTS on AI Risk Management stating that 'Risks covered include both risks to health and safety and risks to fundamental rights which can arise from AI systems, with impact for individuals, organisations, market and society. This document also defines methods that can be used to determine if a package of risk management measures associated with an AI system will be able to ensure that certain risks arising from that product or system are identified, monitored, and managed, leading to an acceptable level of risk.' Available at: https://standards.cencenelec.eu/ords/f?p=205:110:::::FSP_PROJECT,FSP_LANG_ID:79438,25&cs=126AEABA70EBCF2433A6A5472A8FD6F84 accessed 14.01.2026.

99 Marion Ho-Dac, 'Considering fundamental rights in the European Standardisation of artificial intelligence: nonsense or strategic alliance? in Kai Jacobs (ed) Joint Proceedings EURAS & SIIT 2023 (Verlag Gunter Mainz 2023)

21 Finally, in line with the need for expertise recalled in *ESMA*, the limited competences of ESOs in the fundamental rights domain should be highlighted, as acknowledged by the Commission itself,[100] in combination with the time and resources required to provide the contextual and proportionality-based guidance that fundamental rights protection requires. In this regard, the recent Memorandum of Understanding between ESOs and the European Union Agency for Fundamental Rights (FRA)[101] represents a significant step aimed at introducing fundamental rights expertise into HTS drafting process. While such initiative should be welcomed, both as a partial corrective to the overrepresentation of AI industry actors[102] and as a means of fostering a more balanced consideration of rights-related issues, it does not overcome the inherent legal limitation characterising stakeholder involvement inthe standardisationprocess. As consistently emphasized by legal scholars,[103] under current framework, stakeholders have only limited tools to shape the process. Consequently, even when their participation is formally provided for, their possibilities to influence the substance of HTS remains structurally constrained. Accordingly, although an increased engagement of fundamental rights actors is normatively desirable and may partially enhance transparency,[104] it does not address the structural elements that call into question the appropriateness of relying on HTS for the compliance of AI systems with high implications for fundamental rights.

I. Limits and Prospects of the Compensatory Mechanisms.

22 The evaluation of the impossibility of delivering HTS properly protecting fundamental rights has led to the provision on common specifications to be adopted by the EU Commission,[105] via implementing acts, as a fall-back mechanism when fundamental rights concerns are insufficiently addressed. Considering the current state-of-art, this mechanism also suffers from ambiguity, for two main reasons: (i) the threshold of sufficiency in safeguards for fundamental rights that would trigger the adoption of common specifications is not clarified in the Regulation; (ii) the procedural adoption of common specifications relying on the new Excellence Hub on Standardisation, which could raise criticisms similar to the ones related to HTS dealing with fundamental rights.[106]

23 Firstly, like HTS, the common specifications have been introduced as technical tools primarily for products and services.[107] At this stage, the Commission is expected to set up a horizontal approach and to establish the criteria and the processes to define the conditions under which common specifications are required, instead of HTS.[108] Notably, common specifications are not a specific mechanism of the AI Act, they appear in other legislative acts which have a prominent technical or sectoral nature. In

100 See Annex II, point 1 of Implementing Decision (n 51).

101 CEN-CENELEC, 'CEN and CENELEC Sign a Memorandum of Understanding with FRA' (*CEN-CENELEC*, 20 January 2026) https://www.cencenelec.eu/news-events/news/2026/press-releases/2026-01-19-mou-with-fra/ accessed 23.01.2026.

102 See *inter alia*: Mélanie Gornet, Winston Maxwell, 'The European approach to regulating AI through technical standards' (2024) 13/3 Internet Policy Review.

103 The Standardisation Regulation stipulates that ESOs must encourage and facilitate the appropriate representation and effective participation of all relevant stakeholders in their technical work, specifically Annex III identifies the categories of Organisations that are entitled to engage in the standardisation process. Yet, the comments and the opinions issued by these stakeholders throughout the drafting phases are purely consultative, with no binding effect on the ESOs, this limitation is coupled with the absence of formal voting rights. See n.58 and *inter alia* Morten Kallestrup, ' Stakeholder Participation in European Standardization: A Mapping and an Assessment of Three Categories of Regulation' (2017) 44 (4) Legal Issues of Economic Integration 381; Mariolina Eliantonio, 'Private Actors, Public Authorities and the Relevance of Public Law in the Process of European Standardization' (2018) 24 (3) European Public Law 473; Mariolina Eliantonio, Annalisa Volpato, 'The European System of Harmonised Standards. Legal Opinion for ECOS (2022), <: https://ssrn.com/abstract=4055292. or http://dx.doi.org/10.2139/ssrn.4055292> accessed 24.01.2026.

104 Stakeholders participating in the standardization process can have access to working documents of technical bodies, under specific circumstances. See CEN-CENELEC Guide 25-The concept of Cooperation with European Organizations and other stakeholders. Edition 3, updated version January 2026 <https://www.cencenelec.eu/media/Guides/CEN-CLC/cenclcguide25.pdf> accessed 25.01.2026.

105 Art. 41 of the AI Act.

106 Marta Cantero Gamito, Christopher Marsden, 'Artificial intelligence co-regulation? The role of standards in the EU AI Act' (2024) 34 International Journal of Law and Information Technology.

107 See, for example, common specifications on diagnostic medical devices Commission Implementing Regulation (EU) 2022/1107 of 4 July 2022 laying down common specifications for certain class D in vitro diagnostic medical devices in accordance with Regulation (EU) 2017/746 of the European Parliament and of the Council OJ L 178 pp. 3-56; or see Art. 27 (2) of Cyber Resilience Act, Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) OJ L 2847.

108 New Standardisation Strategy (n 63), p.5.

the AI Act, their adoption is foreseen when HTS fail to sufficiently address fundamental rights concerns. In this regard, the Regulation does not specify what constitutes a sufficient level of protection of fundamental rights, nor does it clarify whether common specifications will be adopted before or after HTS are referenced in the Official Journal.

24 Secondly, according to the latest Standardisation Strategy,[109] in the development of common specifications, the Commission would leverage the Excellence Hub, aimed at enhancing cooperation in the existing standardisation expertise within the Commission, EU agencies and Joint Undertakings. It could thus be expected that the fundamental rights protection will be not the core of its activities, unless a proper and specific expertise is included.

25 Another potential compensatory mechanism could be the Fundamental Rights Impact Assessment (FRIA),[110] which requires deployers of certain high risk-high system to assess potential impacts on fundamental rights, prior to deployment. Undoubtedly, the FRIA provision enhances fundamental rights protection; however, its subjective and material scope was significantly narrowed during the trialogue,[111] compared to the initial proposal by the EU Parliament.[112] As a result, it applies only to a limited subset of deployers, differently from HTS established for all high-risk providers.

26 In sum, although the Commission could formally exercise procedural controls over AI-HTS, the lack of a clear and precise mandate to ESOs raises serious reservations about its lawfulness under the delegation doctrine, as well as on the adequacy of HTS as tools for managing risks to fundamental rights. Furthermore, neither the fallback mechanism of common specifications nor the FRIA obligations for deployers can fully compensate for these structural shortcomings. This criticism is further compounded by the limited judicial reviewability of HTS.

II. HTS Limited Judicial Reviewability

27 The hybrid legal nature of HTS presents significant challenges for its judicial review, as extensively pointed out by legal scholars.[113] These are particularly relevant in the realm of fundamental rights protection. Indeed, the Court has expressly recognised that HTS, once referenced in the Official Journal, form part of the EU law and produce legal effects, thus sustaining its interpretative jurisdiction on HTS under Article 267 TFEU.[114]

28 However, the CJEU has consistently held that HTS are acts of ESOs and are not of EU institution, thus restraining the possibility of direct actions for annulment,[115] under Article 263 TFEU, which is one of the main judicial means to ensure fundamental rights protection.[116] The legal status of HTS as non-institutional acts precludes them from being categorized as reviewable acts *per se*. Nonetheless, a procedural pathway for judicial review exists via an action for annulment contesting the Commission's decision to refer to HTS in the Official Journal. However, even in this case, the *locus standi* of private parties would be problematic.[117] As non-privileged

109 ibid.

110 Art. 27 of the AI Act, see: Gianclaudio Malgieri, Cristiana Santos, 'Assessing the (Severity of) Impacts on Fundamental Rights' (2024) Computer Law & Security Review, 56.

111 Art. 27 firstly establishes an obligation on the deployer, rather than on provider, secondly it provides an exception of high-risk AI systems intended to be used in the critical infrastructure and used for public services, which could be derived by Recital 96. In addition, only AI systems in the public sector, for credit worthiness assessment and insurance risk assessments are captured in the scope. For an overview on the differences between risk management in high-risk conformity procedure and FRIA see: Pier Giorgio Chiara, Federico Galli, 'Normative Considerations on Impact Assessments in EU Digital Policy' (2024), 1 Rivista di diritto dei media, 85.

112 In the amendment tabled by Parliament the provision would be applicable to deployers of all high-risk systems listed in Annex III, Amendment 413, P9_TA (2023)0236, adopted 14.06.2023.

113 See: Analisa Volpato, Mariolina Eliantonio, 'The Contradictory Approach of the CJEU to the Judicial Review of Standards: A Love–Hate Relationship?', in Annalisa Volpato and Mariolina Eliantonio, The Legitimacy of Standardisation as a Regulatory Technique (Edward Elgar Publishing 2020); Carlo Tovo, 'Judicial Review of Harmonized Standards: Changing the Paradigms of Legality and Legitimacy of Private Rulemaking under EU Law' (2018) 55 Common Market Law Review 1187. Mariolina Eliantonio, 'Alternative Forms of Regulation: Are They Really "Better" Regulation?: A Case Study of the European Standardization Process' (2017) 19 European Journal of Law Reform 141, 151; Robert van Gestel, Hans Wolfgang 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.

114 Case C-613/14 *Elliott* para 47.

115 Annalisa Volpato, 'The harmonized standards before the ECJ: James Elliott Construction' (2017) 54 Common Market Law Review 591.

116 Interestingly, from quantitative assessment, 1/3 of action for annulments lodged before Grand Chamber and related to fundamental rights regards rightly the effective judicial protection, see Giulia Gentile, 'The Power of Procedure: Fundamental Rights in the Action for Annulment before EU Courts' in Melanie Fink (ed), *Redressing Fundamental Rights Violations by the EU* (Cambridge University Press 2024).

117 Mariolina Eliantonio, 'Judicial Control of the EU Harmonized Standards: Entering a Black Hole?' (2017) 44 Legal Issues of

actors, if private parties were to lodge an action for annulment, they would be required to prove an individual and a direct concern, which is hampered by the restrictive *Plaumann* formula,[118] constantly recalled by the CJEU also in cases concerning potential fundamental rights infringements.[119] It stands to reason that mandatory participation in the procedure leading to the controversial act would allow for the possibility of challenging it, following the *Cofaz* ruling.[120] However, even for private parties participating in the standardisation procedure to HTS, the difficulties in proving the individual and direct concern persist. In the *Schmoldt* case,[121] the Court has clarified that the applicants' participation in the process leading to the adoption of the HTS does not make them individual concerned *per se,* unless the legislation establishes a specific individual procedural guarantee. In the same vein, the Court has stated that an association representing the collective interests of a category cannot be considered individually concerned under Article 263(4) by a measure affecting the general interests of the represented category, and it is not entitled to bring an action for annulment on behalf of its members,[122] where they may not do so individually, unless procedural rights are granted or its interests are affected.[123] It may be expected that the Court would adopt a similar approach in future direct challenges by private parties to AI-related harmonised standards or Commission implementing decisions, even on fundamental rights protection.

29 An alternative possibility for an action for annulment would be the recourse to the "regulatory act" exception within the meaning of Article 263(4) TFEU, which would require the sole demonstration of a direct concern when no further implementing measures are needed.[124] In this regard, in the *Global Garden* case,[125] the Court has affirmed that the Commission decisions to publish HTS are acts of general application against which an action for annulment may be brought. Following the *Global Garden* isolated opening, private parties could file a case for Commission procedural infringements of Regulation on 1025/2012 on standardisation or for non-compliance with the essential requirements established in the AI Act. On these hypotheses, the abovementioned lack of precise criteria and procedural guidance in both the AI Act and the Standardisation Request significantly hinders the possibility of establishing a breach of the essential requirements established in the legislative act, which refer to fundamental rights only in vague and general terms. More relevantly, even if the Commission implementing decisions on HTS reference could be labelled as a "regulatory act," the need for transposition in national standardisation systems could be considered an implementing measure, thus excluding the possibility of relying on the relaxed *locus standi* requirements recognized in such scenarios.[126]

30 It could be inferred that the likelihood of private parties clearing the admissibility threshold in action for annulment is diminished, even without accounting for the limited substantial judicial review[127] that will be conducted in an admissible action.

31 The less intricate possibility to challenge HTS through an indirect preliminary ruling on the validity could be considered. In this regard, substantial and procedural reflections should be made. Firstly, a possible preliminary question to the CJEU would be sent by a national court. This implies that the question(s) would be drafted by national court(s), which would decide its contents, with limited influence for the applicants in the national procedure as well as in the EU proceedings. Indeed, in principle, this judicial procedure aims to ensure uniformity of EU law rather than offer an alternative judicial remedy.[128]

Economic Integration 395.

118 Case C- 25/62 *Plauman v Commission* (1963) C:1963:17 on the admissibility the Court stated that persons other than those to whom a decision is addressed may only claim to be *individually* concerned if that decision affects them because of certain attributes which are peculiar to them, or by reason of circumstances in which they are differentiated from all other persons and by virtue of these factors distinguishes them individually.

119 Case C-565/19 *Armando Carvalho et al. v Parliament and Council* (2021) P EU:C:2021:252, para.48.

120 Case C- 169/84 *Cofaz v Commission* (1986) EU:C:1986:42, para. 30.

121 Case T- 264/03 *Schmoldt et al. v Commission* (2003) EU:T:2004:157.

122 Ibid, para 127.

123 See n 117, p. 402-403.

124 Roberto Mastroianni, Andrea Pezza 'Striking the right balance: limits on the right to bring an action under Article 263(4) of the Treaty on the functioning of the European Union' (2016) 31/4 American University International Law Review 743.

125 Case T-474/15, *Global Garden v Commission*, T:2017:36, para 60.

126 See n 117.

127 Case T- 201/04 *Microsoft v Commission* (2007) EU:T:2007:289, para 85 and cited case-law.

128 Lucia Lopez Zurita, 'Fundamental Rights Complaints in the Preliminary Reference Procedure' in *Melanie Finck (eds). Redressing Fundamental Rights Violations by the EU* (Cambridge University Press 2024).

32 It follows that the long-standing limited judicial reviewability of HTS significantly affects the effective judicial protection of fundamental rights, thus eroding the rule of law, evoked by CJEU in one of its latest ruling on HTS[129] and recalled in the first recital of the AI Act itself.

D. Conclusions

33 The AI Act's reliance on HTS to manage risks to fundamental rights in high-risk scenarios lies at the heart of the broader debate on the appropriate legal tools for addressing the multifaceted challenges posed by AI. In this light, it reflects the underlying tension between the two goals of the Regulation: increasing the well-functioning of the internal market and safeguarding fundamental rights.

34 The risk-based approach seeks to reconcile these objectives by introducing a layered regulatory framework that incorporates soft and hybrid instruments, with HTS playing a key compliance role. While HTS have long been foundational in facilitating market harmonisation, their adequacy for ensuring fundamental rights protection is highly debatable.

35 This contribution has examined the legal and structural limitations of AI HTS in this domain, focusing on high-risk cases. It has emerged that the delegation of delicate normative tasks to private standardisation bodies, without a clear and detailed mandate risks exceeding the boundaries of the EU's delegation doctrine. The vague references in the AI Act and the Standardisation Request fail to provide the necessary legal clarity, potentially opening the door to a discretionary power exercised by private third parties in the delicate domain of fundamental rights. Moreover, the procedural safeguards currently in place, such as Commission oversight and emergency fallback mechanisms like common specifications, appear insufficient to compensate for these shortcomings. Similarly, the Fundamental Rights Impact Assessment (FRIA), while valuable, is limited in scope and cannot substitute for a robust and rights-oriented assessment to be ensured by design and by providers. The limited judicial reviewability of HTS, highlighted by legal scholars, remains a critical structural weakness, raising serious concerns about effective fundamental rights protection, linked to the rule of law within the AI regulatory framework.

36 It should be noted that a revision of the Standardisation Regulation is expected by the second quarter of 2026. However, in line with the Standardisation Strategy, it is not expected to mark a revolution of HTS, which will remain strongly a market-oriented instrument.[130] The recourse to common specifications by EU Commission could be a potential alternative, but their effectiveness will depend on their implementation and the inclusion of rights-based expertise in its adoption procedure.

37 Considering that the fundamental rights protection is both an AI-risk dimension and a prominent objective of the Regulation, it emerges that alternatives to HTS are required.

38 Looking ahead, the issuance of specific Guidelines by the Commission, as already envisaged within its mandate,[131] constitutes a prospective pathway to be further investigated. Notably, the adoption of Guidelines concerning the identification and the management of risks to fundamental rights in high-risk scenarios could provide an interpretive framework, thereby streamlining the *ex ante* risk assessment mandated for providers. The recourse to Guidelines has been consistently used in mature EU legal domain, though their function varies, triggering a presumption of legality, as in the competition law,[132] or function as a guidance, such

129 Case C-588/21 P *Public Resources Org v Commission* (2024) EU:C:2024:201, para 81.

130 See Call for Evidence for an Impact Assessment, European Commission, Ares (2025) 4981369 - 23/06/2025

131 See Art. 96 (1), let. a) of AI Act which establishes that the Commission is expected to develop guidelines on the practical implementation of the Regulation, in particular on the application of the requirements and obligations referred to in Articles 8 to 15, thus including articles to be covered by HTS.

132 The EU Commission issues Guidelines on diverse topics in the competition law domain, including on the applicability of the Articles 101 and 102 of TFEU which represents its pillars. The Guidelines provide guidance and analytical framework to undertakings and reflect the EU courts' caselaw evolution, as emerged from the latest adopted Guidelines on horizontal cooperation agreements. See European Commission, Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal cooperation agreements, C(2023)4752 final. It should be noted the role played by the Commission in the enforcement competition architecture, which grants a relevant value to related soft law instruments, specifically trough the so called 'safe harbour' which preclude a finding of a competition infringement and/or make it unnecessary to assess market circumstances in order to find a conduct lawful if certain pre-determined conditions established in the Guidelines are met. See *inter alia:* Lorenzo Federico Pace *European competition law: the impact of the Commission's Guidance on article 102* (Edward Elgar 2011); Zlatina Georgieva, 'Soft Law in EU Competition Law and its Judicial Reception in Member States: A Theoretical Perspective'(2015), 16/2 German Law Journal 223; Martine de Koning, Jelle Blom, 'The New European Block Exemption Regulation on Vertical Agreements: Renewal of the Safe Harbor for Vertical

as in the aforementioned data protection field.[133] This latter case seems to offer a particularly salient model for the AI Act. In this vein, the precedent set by Commission Guidelines on prohibited AI practices[134] demonstrates the possibility to support the interpretation and the implementation of AI Act key provisions, underscoring its relationship with EU law *acquis*, including fundamental rights protection, while orienting AI operators. Relevantly, the Guidelines on prohibited AI practices suggest criteria and analytical framework to assess the potential significant harms to fundamental rights for certain AI systems. Ultimately, the Guidelines adoption process would facilitate the integration of diverse stakeholders' inputs, as established under the Better Regulation,[135]while leveraging the expertise of the Advisory Forum members[136], including ESOs, to ensure coherence and synergy with HTS, which would play a supplementary role in fundamental rights domain.[137]

39 As the AI Act enters in its critical implementation phase, the EU must ensure that it remains both technologically resilient and properly protective for fundamental rights, to serve its objectives and build up a human-centric and trustworthy AI ecosystem.

Agreements Such as Franchise Agreements and a New Era on What Is (and Is Not) Permitted on Digital Commerce Within the European Union' (2023) 23/3 Franchise Law Journal, 295.

133 See n 96. In data protection, the Guidelines have been issued by European Data Protection Board (EDPB), according to its mandate, as established by Art.70 (1) let.d) of Regulation (EU) 2016/679. Differently, the European Artificial Intelligence Board (EAIB) can issue recommendations, while assisting the Commission for guidance documentation, as derived from art. 64 of the AI Act.

134 European Commission, Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act), C(2025) 5052 final.

135 See Better Regulation Guidelines, SWD (2021) 305 final.

136 Art. 67 of the AI Act. Particularly, art. 67 (3) establishes that ESOs together with the Fundamental Rights Agency and ENISA shall be permanent members of the Advisory forum.

137 See n 134 and Marion Ho-Dac, 'The EU AI Act and the challenge of protecting fundamental rights' (2025) 62 Common Market Law Review 1299.

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.

jipitec

Journal of
Intellectual Property,
Information Technology,
and Electronic Commerce
Law

www.jipitec.eu