The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy

Marco Almada & Anca Radu

Abstract Over the last few years, artificial intelligence (AI) technologies have become embedded in various domains of social life, prompting legislative efforts at the national and international levels. In the European Union (EU), this drive for legislation has been reflected in various legal instruments, notably the proposed AI Act, which is expected to become a global standard through the Brussels Effect. This article argues that, while the AI Act is likely to produce a Brussels Effect of its own, such an outcome will be accompanied by a *side effect*: undermining the EU's ambition of spreading not just legislative text but values in the governance of AI. Since the AI Act is patterned after EU product safety legislation, its provisions supply limited protection of some of the values EU policy intends to protect, such as the protection of fundamental rights. These shortcomings are compounded by the EU's active efforts to shape alternative instruments, such as the Council of Europe's proposed convention on AI, along the lines of the AI Act. As a result, the diffusion of the AI Act as a global standard will have consequences for the EU policy agenda on AI and the conceptualization of the Brussels Effect.

Keywords artificial intelligence; European Union; Council of Europe; Brussels Effect; regulatory competition

Marco Almada is a Researcher at the Department of Law, European University Institute, working on technology neutrality and specificity in AI regulation. Email: Marco.Almada@eui.eu. Website: www.marcoalmada.com. ORCID: https://orcid.org/0000-0002-0127-6549

Anca Radu is a Researcher at the Department of Law, European University Institute, working on AI applications in the judiciary and their impact on human rights, democracy, and the rule of law. Email: Anca.Radu@eui.eu. LinkedIn: www.linkedin.com/in/raduanca. ORCID: https://orcid.org/0000-0003-2732-872X.

Contents

Artificial Intelligence (AI) has recently become a central topic in the European Union (EU)'s digital regulation agenda. The European Commission has repeatedly emphasized the need to foster the adoption of AI technologies in the EU,[1] and recent legislative reforms, such as those dealing with the EU data protection framework[2] and other aspects of the digital single market,[3] have included provisions focused on AI. These provisions coexist with the apparent crown jewel of the EU regulatory approach: the AI Act,[4] a horizontal legal instrument which intends to foster the adoption of safe, trustworthy, and human-centric AI systems in the EU.

The AI Act was initially proposed in April 2021 and is currently undergoing the ordinary legislative procedure. It reflects a two-pronged EU AI strategy, which seeks to turn the EU into a "world-class AI hub" and ensure the safety and trustworthiness of AI systems used within the Union.[5] Within this scheme, the EU regulatory framework for AI is expected to follow a value-based approach. More than that: it is expected to promote European values worldwide.[6] But the development of AI technologies is primarily led by a handful of corporations based, for the most part, outside the EU.[7] How is a legal instrument internal to the EU legal order supposed to have a global impact on the spread of EU values for AI governance?

One of the mechanisms posited for that global influence is the so-called Brussels Effect.[8] Because the EU single market comprises hundreds of millions of consumers with considerable spending power and the companies that attend to these consumers, access to that market can be attractive to businesses. This attractiveness means that, under certain circumstances, companies might cater to stringent EU standards in their global operations, while other jurisdictions might pattern their own rules after the EU approach. Given the peculiarities of AI-related markets, there has been some debate on whether the AI Act will give origin to a Brussels Effect.[9]

In this paper, we argue that the AI Act's likely Brussels Effect creates the risk of a strong *side effect*: the spread of the Act as a regulatory template for the world might undermine many of the European values the EU AI strategy is meant to promote. On the policy side of things, the risk of a Brussels Side Effect maps an internal tension within EU digital policy, as promoting the AI Act as a global standard is likely to spread many of the shortcomings associated with the EU regulatory standard. On the theoretical side of things, the risk of a side effect appears *because* the EU regulation is strict and not despite it. Given that stringency is one of the necessary conditions for the Brussels Effect, this means that, at least in some circumstances, the very existence of such an effect plays against some of the policy goals said effect is expected to promote.

To make these interconnected points, the paper proceeds as follows. In Part A *infra*, we provide an overview of the AI Act, showing that some of its aspects were designed to increase the

[1] See, generally and as an example, European Commission, *Fostering a European Approach to Artificial Intelligence*, No. COM/2021/205 final (2021).
[2] Paul Nemitz, Constitutional democracy and technology in the age of artificial intelligence, 376 PHIL. TRANS. ROYAL SOC'Y A 8–10 (2018).
[3] See generally Troels Krarup & Maja Horst, *European Artificial Intelligence Policy as Digital Single Market Making*, 10 BIG DATA & SOC'Y 20539517231153811 (2023).
[4] 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 (2021).
[5] Commission, *supra* note 1, at 1.
[6] *Id.* at 7.
[7] See generally Nur Ahmed et al., *The Growing Influence of Industry in AI Research*, 379 SCIENCE 884 (American Association for the Advancement of Science Mar. 2023).
[8] See generally Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press Mar. 2020).
[9] See Part B.I *infra*.

probability of a Brussels Effect in AI governance but that the overall regulatory arrangement has considerable limitations when it comes to the protection of fundamental rights, democracy, and the rule of law. In Part B, we argue that these shortcomings are likely to be spread globally, as these issues are not enough to prevent the emergence of a Brussels Effect for the AI Act. And, as the shortcomings of the AI Act gain global traction, this success in exporting regulatory standards can lead to a reduced level of fundamental rights protection. Such a concern is particularly salient in the context of the Council of Europe (CoE)'s proposed convention on human rights, democracy, and the rule of law, which we examine in Part C. While the convention could provide an escape valve to the limits of the AI Act regarding fundamental rights, the EU's current position in CoE negotiations threatens this potential by shaping the convention into a vehicle for the diffusion of the AI Act approach. The pursuit of a Brussels Effect in AI is, therefore, put before the values the effect is expected to promote. Finally, we conclude the paper with some remarks on the impacts of this phenomenon on AI regulation and the study of the Brussels Effect.

A The EU Approach to AI Regulation

AI regulation in the EU, as mentioned *supra*, is a two-headed beast. On the one hand, it follows the market imperative at the core of the European project: the AI Act is expected to create a single market for AI,[10] preventing market fragmentation and supplying market actors with the legal certainty they need to operate.[11] On the other hand, it is a value-laden instrument that restricts access to the EU single market to "trustworthy" AI systems compliant with Union values, notably the protection of fundamental rights.[12] The text of the AI Act reflects a balance between those two aims.

In crafting such a balance, the EU must observe certain constraints. Some of these constraints are constitutional: unlike a sovereign state, the EU can only legislate within the limits of the competencies conferred to it by its Member States.[13] Most of these competencies are sector-specific, allowing the EU to act in a specific domain, such as environmental protection or antitrust. But, given its goal of avoiding market fragmentation, the AI Act is designed as a horizontal instrument, that is, as a regulation that applies to all AI systems.[14] And the protection of fundamental rights does not, in itself, provide a basis for EU legislation.[15] As a result, the AI Act shoehorns the protection of fundamental rights into the most general legal basis available for legislation: Article 114 of the TFEU,[16] which provides a general competence for approximating rules on the internal market.[17]

[10] Recital 5 AI Act: 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 (2021) [hereinafter AI Act].
[11] Recital 6 AI Act.
[12] Recital 1 AI Act.
[13] Article 5(2) TEU: Consolidated version of the Treaty on European Union, 2016 OJ (C 202) 13.
[14] COM(2021) 206 final at 3.
[15] Article 51(2) CFR: Charter of Fundamental Rights of the European Union, 2016 O.J. (C 202) 389.
[16] Consolidated version of the Treaty on the Functioning of the European Union, 2016 OJ (C 202) 47.
[17] For an overview of the potential legal bases available for horizontal AI regulation, see Pieter Van Cleynenbreugel, *EU By-Design Regulation in the Algorithmic Society: A Promising Way Forward or Constitutional Nightmare in the Making?*, *in* CONSTITUTIONAL CHALLENGES IN THE ALGORITHMIC SOCIETY 202, 209–12 (Hans-W. Micklitz et al. eds., Cambridge University Press 2021).

To the extent that the AI Act relies on the EU competence to regulate the single market,[18] it must be framed as an instrument that promotes market integration.[19] While the EU has a vast repertoire of approximation measures, the AI Act settles upon a specific method: product safety regulation.[20] By adopting this frame, the EU can benefit from decades of expertise with its previous product safety instruments, which have become a global standard.[21] And, by drawing upon the mechanisms for EU-wide coordination in product risks, the EU can—at least in theory—avoid the enforcement issues currently plaguing its data protection framework.[22] The AI Act is, therefore, a reasoned response to the goals and constraints of the EU AI strategy.

In the following pages, we overview how the EU adapted its product safety approach to AI and then discuss some of the shortcomings of that approach. These shortcomings hinder the pursuit of goals beyond the original product safety framework, particularly those connected to fundamental rights protection. Hence, the AI Act, despite its horizontal ambitions, is insufficient to address the value-setting ambitions of EU policy.

A.I The AI Act in a Nutshell

Any product regulation requires a clear definition of its target product, and the AI Act is no different. In line with a growing international consensus,[23] the Act's main regulatory target is the *AI system*, which is defined as a software system, developed with one or more techniques associated with AI,[24] that generates outputs such as predictions, recommendations, or decisions.[25] Some of the Act's provisions specify technical requirements for these systems. Others lay down obligations for the various actors involved in placing these systems on the EU market, putting them into service, or using them. But all these obligations are cast in terms of the AI system perceived as a discrete product.

The AI Act relies on a risk-based approach to govern such AI systems. Under the proposed framework, risks are subject to a top-down classification, in which the EU legislator defines three categories of risks and specifies which applications of AI fall into each category.[26] Under a

[18] According to Recital 2 AI Act, the provisions on real-time biometric identification systems—and only those—are grounded on Article 16 TFEU, which establishes data protection as an EU competence. In the Parliament compromise text, the newly-introduced Recital 2a states that the entire regulation is also based on Article 16 TFEU: Brando Benifei & Ioan-Dragoş Tudorache, *Report on the Proposal for a Regulation of the European Parliament and of the Council on Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD))*, No. PE731.563v02-00 (May 2023). This expanded role for Article 16 TFEU is reflected in some new provisions introduced by the Parliament text, but the overall framework remains that of product safety—and thus Article 114 TFEU still constrains the general shape of the AI Act.

[19] Action under Article 114 TFEU must have *some* connection with the market approximation goal of that treaty provision, even if the ECJ tends to allow a broad scope for such approximation measures: Case C-376/98, *Federal Republic of Germany v European Parliament and Council of the European Union*, 2000 E.C.R. I–08419, paras. 106–108.

[20] On the Commission rationale leading to the product safety frame for the AI Act, see Gabriele Mazzini & Salvatore Scalzo, *The Proposal for the Artificial Intelligence Act: Considerations around Some Key Concepts* 2–5 (Ca 'Foscari University Nov. 2021).

[21] Charlotte Siegmann & Markus Anderljung, The Brussels Effect and Artificial Intelligence: How EU Regulation Will Impact the Global AI Market 78 (Aug. 2022).

[22] See generally Gloria González Fuster et al., *An Empirical Study of Current Practices under the GDPR* (Jun. 2022).

[23] See, e.g., OECD, Recommendation of the Council on Artificial Intelligence (May 2019); UNESCO, The Recommendation on the Ethics of Artificial Intelligence (Feb. 2020).

[24] Annex I AI Act.

[25] Article 3(1) AI Act. Note that both the Council and the European Parliament have proposed to eliminate the reference to Annex I, so the overall form of this definition is still subject to change.

[26] On the difference between this approach and the risk-based approaches adopted in other EU digital instruments, see generally Giovanni De Gregorio & Pietro Dunn, *The European risk-based approaches: Connecting constitutional dots in the digital age*, 59 COMMON MKT. L. REV. 473 (2022).

precautionary approach, some applications of AI are prohibited because the risks they pose to the health, safety, and fundamental rights of individuals are deemed unacceptable.[27] The majority of the other AI systems are not considered to pose a substantive risk by the mere virtue of their intended application.[28] The AI Act does not introduce specific rules for such systems,[29] leaving their governance to voluntary codes[30] and sector-specific legislation, such as the General Product Safety Directive.[31] Instead, it devotes most of its substantive provisions to applications deemed to pose a high risk to health, safety, and fundamental rights.[32]

High-risk AI systems are governed by rules derived from the New Legislative Framework for product safety.[33] Under such an approach, the providers[34] of AI systems must ensure that the system meets specific technical requirements before the system can be placed on the EU single market, put into service, or otherwise used.[35] Providers themselves usually evaluate conformity with such requirements through internal controls, but external assessment may sometimes be required.[36] But, even if internal controls are sufficient *de jure*, providers might find themselves *de facto* required to rely on external forms of validation, such as certification mechanisms or conformity to harmonized technical standards commissioned by the Commission,[37] in order to ensure full coverage of the legal requirements, which provide abstract descriptions of the outcomes that the technical measures must ensure.

In the original Commission text, the risk profile of an AI system is based on its intended application. Such an arrangement, however, is ill-suited to models that can be used for various tasks, such as the large language models that have been popularized in 2023.[38] This inadequacy follows from the fact that said models are intended as components for other AI systems. For example, it has been suggested that systems such as ChatGPT can support public-sector bodies in their interactions with citizens.[39] In such circumstances, the provider of the AI system would be the legal or natural person that repurposes this general system for a specific purpose, but that provider might lack the means

[27] Article 5 AI Act. On the consumer protection roots of this provision, see generally Catalina Goanta, *Regulatory Siblings: The Unfair Commercial Practices Directive Roots of the AI Act* (Jan. 2023).

[28] Between 85% to 95% of the AI systems in the EU single market, under Commission estimates: Impact Assessment Accompanying the 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, No. SWD(2021) 84 final 71 (Apr. 2021).

[29] Article 52 AI Act specifies transparency rules for certain kinds of AI systems, such as those used for emotion recognition, which apply regardless of the risk level ascribed to the system.

[30] Article 69 AI Act.

[31] Recital 82 AI Act.

[32] Article 6 AI Act specifies two kinds of high-risk AI systems. An AI system is a high-risk AI system if it is a product covered by one of the pieces of harmonizing product safety legislation listed in Annex II, or a component of such a product. Otherwise, an AI system is a high-risk system if it is intended for one of the applications listed in Annex III of the Act.

[33] For an overview of the New Legislative Framework and its application in the AI Act, see Michael Veale & Frederik Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach*, 22 COMPUT. L. REV. INT'L. 97, 102–6 (2021).

[34] Other actors, such as importers and the users of AI systems, are subject to certain obligations: Article 24–29 AI Act. But the bulk of the Act is directed at providers, even if the Parliament compromise text proposes an expansion of the list of obligations under Article 28 AI Act.

[35] Article 10–15 AI Act.

[36] Article 43 AI Act.

[37] See Martin Ebers, *Standardizing AI - The Case of the European Commission's Proposal for an Artificial Intelligence Act*, *in* THE CAMBRIDGE HANDBOOK OF ARTIFICIAL INTELLIGENCE: GLOBAL PERSPECTIVES ON LAW AND ETHICS 338 (Larry A. DiMatteo et al. eds., Cambridge University Press 2022).

[38] See generally OECD, *AI Language Models: Technological, Socio-Economic and Policy Considerations*, No. DSTI/CDEP/AIGO(2022)1/FINAL (Organisation for Economic Co-operation and Development Apr. 2023).

[39] See generally General Secretariat of the Council of the European Union, *ChatGPT in the Public Sector – Overhyped or Overlooked?* (Apr. 2023).

to effect technical changes on the tools they use.[40] The effectiveness of the technical requirements described *supra* would, therefore, be contingent on the technical decisions made by the provider of the general-purpose system used in a high-risk application, which seldom account for all the risks in a particular high-risk context.

To address these shortcomings, the Council General Approach[41] and the political compromise arrived at by the European Parliament[42] both include rules on general-purpose AI systems that can be adapted to various tasks.[43] While the regulatory instruments proposed by each institution differ in their specifics, they both share the same overall approach: imposing on the providers of (some) general-purpose AI systems obligations regarding the mitigation of foreseeable risks and transparency about the system. It is likely, therefore, that the final version of the AI Act will feature some form of technical requirements for general-purpose AI, which are unlikely to be as strict as those applicable to high-risk AI.

Conformity to *ex ante* requirements addresses those risks that can be anticipated during system design. But some issues might not be detected beforehand, while others might be consequences of use. To address these gaps in risk response, providers are expected to develop a system of risk management practices for the AI system[44] and collect information about it once it is on the EU market.[45] If any risks are detected—either through the provider's monitoring practices or by the action of market surveillance authorities—providers must take corrective measures[46] or face penalties such as fines[47] or the loss of access to the EU market.[48] So the AI Act tackles the risks associated with AI throughout the entire life cycle of AI systems, from their design to the end of their operation.

A.II The Limits of the AI Act

The outline show in Part A.I *supra* suggests the AI Act is in an excellent position to achieve the goals that prompt its adoption.[49] Its reliance on a product safety framework provides legal certainty, as the providers can rely on the expectations built with previous product safety laws[50]—to which they are already subject in many cases.[51] And the extension of that framework to cover risks to fundamental rights addresses many of the concerns raised by AI applications, especially, but not

[40] On the challenges of targeting the regulation of general-purpose AI, see Marco Almada & Nicolas Petit, *The EU AI Act: Between Product Safety and Fundamental Rights* 10–13 (Dec. 2022).
[41] Council of the European Union, 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 - General Approach, No. 14336/22, art. 4a (Nov. 2022).
[42] Benifei & Tudorache, *supra* note 18, art. 28b.The Parliament text defines "general purpose AI" but does not use it in any binding instruments, focusing its obligations on related concept: the so-called "foundation models".
[43] The Council and the European Parliament are the European co-legislators, which means that a piece of legislation proposed under the ordinary legislative procedure (as is the case of the AI Act) must be approved by both institutions before it can become law. For a guide to the EU legislative procedure, see generally Tiago Sérgio Cabral, *A Short Guide to the Legislative Procedure in the European Union*, 6 UNIO – EU LAW JOURNAL No. 1, 161 (2020).
[44] Article 9 AI Act.
[45] On the requirements for the post-marketing surveillance system, see Article 61 AI Act.
[46] Article 16(g) and 65(4) AI Act.
[47] Article 71 AI Act.
[48] Article 65(5) AI Act.
[49] Commission, *supra* note 4, at 3.
[50] For an overview of the EU product safety framework, see Geraint Howells & Jonathan Watson, *European Consumer Law*, *in* EUROPEAN UNION LAW 723, 735–37 (Steve Peers & Catherine Barnard eds., Oxford University Press 4th ed. 2023).
[51] Article 6(1) AI Act specifies that the high-risk label—and the ensuing regulatory framework—applies to systems already covered by specific product harmonization laws at the EU level.

exclusively, in the public sector.[52] Nonetheless, the AI Act has been subject to extensive critique by scholars[53] and civil society organizations.[54] Why is that so?

A complete presentation of the critiques of the AI Act would exceed this paper's scope. But, for our argument, it is essential to highlight the tension between the fundamental rights aims built into the AI Act's framework and the product safety instruments used to pursue these goals.[55] Within product safety legislation, the risk associated with an adverse event can be calculated, at least in principle: if one measures the likelihood of the event happening and the severity of that event, the value of the risk is the product between these two quantities.[56] Such a definition is ill-suited to capture various risks to fundamental rights, such as those affecting dimensions of fundamental rights that are not amenable to computational representation[57] or those stemming from the cumulative harmful effects of practices that are not very harmful in and of themselves.[58] Therefore, the AI Act's formula of protecting fundamental rights through the same mechanisms used to address health and safety risks runs the risk of neglecting important forms of harm to these rights.

Another line of concern focuses on the actual rules applied to AI systems. While the rules for high-risk AI are extensive, they are formulated in abstract terms. Consequently, their implementation requires extensive interpretation efforts by the providers of AI systems, who become *de facto* responsible for determining how the legal requirements are converted into software requirements.[59] In doing so, they face a technical challenge: expressing the relevant legal requirements as software. Such an expression might be feasible for legal rules that demand little interpretation, but fuzzier rules and legal principles are not so easily represented in computer code.[60] And, because many AI systems are large-scale systems,[61] changing them to fix errors in representation—or to cope with changes in the law—can be a slow process.[62] Reliance on technical measures may thus entrench arbitrary or even wrongful interpretations of the law by the providers of an AI system.[63]

---

[52] See generally FRA, Getting the Future Right – Artificial Intelligence and Fundamental Rights (Dec. 2020).

[53] See generally Veale & Borgesius, supra note 33; Nathalie Smuha et al., A Response to the European Commission's Proposal for an Artificial Intelligent Act 64 (May 2021); Lilian Edwards, Regulating AI in Europe: Four Problems and Four Solutions (Ada Lovelace Institute Jan. 2022); Vera Lúcia Raposo, Ex machina: preliminary critical assessment of the European Draft Act on artificial intelligence, 30 INT'L J.L. & INFO. TECH. 88 (2022).

[54] See, e.g., EDRi et al., An EU Artificial Intelligence Act for Fundamental Rights. A Civil Society Statement. (Nov. 2021).

[55] For more extensive treatments of the expressive limits of the AI Act's risk framework, see generally Almada & Petit, *supra* note 40; ALESSANDRO MANTELERO, BEYOND DATA: HUMAN RIGHTS, ETHICAL AND SOCIAL IMPACT ASSESSMENT IN AI (Springer Nature 2022); Sofia Palmieri & Tom Goffin, *A Blanket That Leaves the Feet Cold: Exploring the AI Act Safety Framework for Medical AI*, 30 EUR. J. HEALTH LAW early access (2023).

[56] See, e.g., Article 7(1)(b) AI Act, which adopts severity and likelihood as guiding criteria for the Commission's delegated power to expand the list of high-risk AI systems under Annex III.

[57] Mireille Hildebrandt, Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning, 20 THEORETICAL INQUIRIES L. 83 (2019).

[58] See generally Burkhard Schafer, Death by a Thousand Cuts: Cumulative Data Effects and the Corbyn Affair, 45 DATENSCHUTZ UND DATENSICHERHEIT - DUD 385 (2021); Hin-Yan Liu et al., Governing Boring Apocalypses: A New Typology of Existential Vulnerabilities and Exposures for Existential Risk Research, 102 FUTURES 6 (2018).

[59] Cleynenbreugel, *supra* note 17, at 203–8; Marco Almada, *Regulation by Design and the Governance of Technological Futures*, EUR. J. RISK REG. FirstView, 3–6 (2023).

[60] Bert-Jaap Koops & Ronald Leenes, Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law, 28 INT'L REV. L. COMPUTS. & TECH. 159, 6–8 (2014).

[61] See generally Simone Vannuccini & Ekaterina Prytkova, Artificial Intelligence's New Clothes? From General Purpose Technology to Large Technical System, No. SWPS 2021-02 (Jul. 2021).

[62] On the temporality of technical change, see generally Lyria Bennett Moses & Monika Zalnieriute, *Law and Technology in the Dimension of Time*, *in* TIME, LAW, AND CHANGE: AN INTERDISCIPLINARY STUDY 303 (Sofia Ranchordás & Yaniv Roznai eds., Hart Publishing 2020).

[63] On technical norms as a source of regulatory entrenchment, see Almada, *supra* note 59, at 8–10.

The AI Act includes a few mechanisms that may provide guidance and avoid arbitrary interpretation by providers, such as the (currently narrow) requirements for external certification and the pervasive role that harmonized standards play in evaluating compliance with the Act.[64] Still, reliance on external actors also has its issues. Technical standards and certification schemes are both produced by private bodies,[65] in which deliberations are framed in technical language and seldom open to the general public.[66] As a result, there are considerable doubts about whether standards-setting organizations and other technical bodies are legitimate parties for specifying norms directed at the protection of fundamental rights, coming both from external observers[67] and from technical decision-makers themselves.[68]

If these and other critiques hold, protecting fundamental rights through the AI Act's product safety framework might be ineffective. The Act might fail to respond to issues that cannot be easily framed in the kind of quantified risk product safety thrives in, and it might fail to address all dimensions of the risks it does detect. Furthermore, the outsized role of opaque private actors in making decisions about codifying fundamental rights means that the AI Act may produce negative outcomes for other public interests, such as democratic governance[69] and the rule of law.[70] The AI Act, meant to protect the EU from the risks associated with AI technologies, may itself run against the many values the EU is expected to uphold.[71] And, in doing so, the Act undermines its very purpose.

B The AI Act as a Global Standard?

Part A *supra* situated the AI Act and its potential shortcomings within the EU legal order. But the Act is not directed solely at producing results within the EU single market. Instead, as discussed in the Introduction, it is expected to position the Union as a global leader in AI. Is such leadership possible if the AI Act provides insufficient protection for fundamental rights and other public values?

At first glance, the answer to this question might seem to be "no". One of the necessary conditions for the Brussels Effect is that the regulation must be *stringent*, such that compliance with it is enough to meet the demands of other jurisdictions. Because sovereign states can establish norms to directly address fundamental rights—and, indeed, are currently doing so[72]—providers of AI

[64] Article 42 AI Act.
[65] Or, in the case of EU harmonized standards, quasi-private ones. See generally Marta Cantero Gamito, *Europeanization through Standardization: ICT and Telecommunications*, 37 Y.B. EUR. L. 395 (2018).
[66] See generally Olia Kanevskaia, Governance of ICT Standardization: Due Process in Technocratic Decision-Making, 45 N.C. J. INT'L L. 549 (2019).
[67] 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 THE LEGITIMACY OF STANDARDISATION AS A REGULATORY TECHNIQUE 1 (Mariolina Eliantonio & Caroline Cauffman eds., Edward Elgar Publishing 2020); Smuha et al., supra note 53, at 54.
[68] For an example, see generally Corinne Cath, The Technology We Choose to Create: Human Rights Advocacy in the Internet Engineering Task Force, 45 TELECOMM. POL'Y 102144 (2021).
[69] See generally Carles Boix, *AI and the Economic and Informational Foundations of Democracy*, *in* THE OXFORD HANDBOOK OF AI GOVERNANCE (Justin Bullock et al. eds., Oxford University Press 2022).
[70] See generally Emre Bayamlıoğlu & Ronald Leenes, *The 'Rule of Law' Implications of Data-Driven Decision-Making: A Techno-Regulatory Perspective*, 10 LAW INNOVATION & TECH. 295 (Routledge 2018).
[71] Article 2 TEU.
[72] See, e.g., the Brazilian draft regulatory framework for AI: Projeto de Lei n° 2338, Senado Federal (2023). For an English-language overview of that proposal, see generally Evangelos Sakiotis et al., *Brazil's Senate Committee Publishes AI Report and Draft AI Law*, INSIDE PRIVACY (Jan. 27, 2023), https://www.insideprivacy.com/emerging-technologies/brazils-senate-committee-publishes-ai-report-and-draft-ai-law/.

systems would need to adopt additional measures to cope with those fundamental rights requirements that cannot be cast in terms of product safety standards. While such a conclusion is reasonable in light of our previous discussion, current analyses of the AI Act lead us to sustain in Part B.I *infra* that a Brussels Effect might happen nonetheless. The limits of the AI Act when it comes to fundamental rights protection are less salient in some applications, and the other requirements for such an effect are still present. So, the AI Act might become a global standard despite any shortcomings of the product safety framework in its new task as a guardian of fundamental rights.

Success in spreading the AI Act's regulatory framework does not, however, automatically lead to success in setting the European approach to AI as a global standard. In Part B.II *infra*, we argue that the opposite is true. Any Brussels Effect from the AI Act is likely to produce a *side effect*: spreading around the world norms that pay insufficient attention to the values the EU is founded on.[73] As other jurisdictions pattern their laws after the AI Act, they will adopt a model that, as seen in Part A *supra*, does not cover all the dimensions of fundamental rights and public interests it is meant to. Furthermore, the global adoption of an insufficient standard of value protection may come back to haunt the EU itself, for example, by restricting the possibility of fixing the AI Act's deficits through international treaties. Under these circumstances, spreading the letter of EU AI regulation can constrain the EU's ability to shape the values guiding the adoption of AI at the European and global levels.

B.I The AI Act's Potential Brussels Effect

From its onset, the AI Act was designed with its worldwide effects in mind.[74] Such a global concern reflects the Commission's ambitions of positioning the EU as a global AI leader[75] and the previous experiences with the impact of EU digital regulation on the laws of other jurisdictions and international treaties.[76] While the EU cannot force other jurisdictions to follow its lead, it can sway their regulatory approaches through various mechanisms. Some of those involve bilateral or even multilateral action, as is the case of the CoE convention on AI we examine in Part C. But, under certain circumstances, the EU can also exercise unilateral influence via the Brussels Effect.[77]

The Brussels Effect is a market-based mechanism for regulatory exportation. Through the soft coercion enabled by its strong internal market, the EU often spreads its regulatory standards even if those are not favored by the EU's trade partners.[78] In its original formulation, the Brussels Effect was seen as a mostly *de facto* phenomenon, in which companies comply with EU standards—even when formally subject to less strict ones—because economic factors push them to do so.[79] But it can also happen as a *de jure* influence, as jurisdictions emulate the EU regulatory approach due to

[73] Article 2 TEU.
[74] On the AI Act as a pioneer in global AI regulation, see Mazzini & Scalzo, *supra* note 20, at 1.
[75] Commission, *supra* note 1, at 4.
[76] BRADFORD, *supra* note 8, ch. 5.
[77] This is not to say that other jurisdictions are merely passive recipients of EU influence. Instead, they modulate reception of EU influences through the lenses of local regulatory frameworks and priorities. See generally Paul M Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771 (2020); Laura Schertel Mendes & Bruno R Bioni, *O regulamento europeu de proteção de dados pessoais e a lei geral de proteção de dados brasileira: mapeando convergências na direção de um nível de equivalência*, 124 RDC 157 (2019); Emmanuel Pernot-Leplay, *China's Approach on Data Privacy Law: A Third Way Between the U.S. and the E.U.?*, 8 PENN ST. J. L. & INT'L. AFF. 49 (2020).
[78] BRADFORD, *supra* note 8, at xiv.
[79] *Id.* at 6.

corporate lobbying,[80] political pressures to catch up with technological change, or other factors.[81] Either way, scholarship on EU regulation has identified five conditions that must be met for policy diffusion through the Brussels Effect.[82]

If the AI Act is to produce a Brussels Effect, it must be benefitted by *market size*.[83] Based on the available evidence, the EU is likely to be a large market for AI systems. The substantial population covered by the EU single market and its wealth make it incredibly attractive to providers of consumer goods based on AI. Similarly, large online platforms are unlikely to forgo access to the millions of users based in EU Member States.[84] And the EU also offers substantial markets for AI systems marketed for business uses and public sector applications.[85] Because conformity with the AI Act is a prerequisite for selling AI systems in the EU single market, the risk of being pushed out of it is likely to be salient for providers of AI systems operating globally.

It is also relatively straightforward to show that the AI Act meets the second requirement for a Brussels Effect: *regulatory capacity.*[86] Because AI is a novel technology, which has undergone significant developments in the last few years,[87] there is little established knowledge on how to regulate AI systems. The EU adopted two strategies to mitigate this general ignorance. First, it has worked to develop extensive expertise in AI. AI technologies were a focal topic in the reform of EU data protection law in the mid-2010s,[88] the AI Act was preceded by the work of a High-Level Expert Group formed by people from academia and industry,[89] and national and EU bodies are hiring AI experts.[90] Second, reliance on the product safety framework allows the EU to rely on decades of expertise to interpret and enforce the AI Act.[91] As such, few jurisdictions[92] have the technical and institutional capabilities available to the EU for AI regulation.[93]

---

[80] *Id.* at 84.

[81] On the pacing problem in law and technology, see generally Gary E. Marchant, *Addressing the Pacing Problem*, *in* THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT: THE PACING PROBLEM 199 (Gary E. Marchant et al. eds., Springer Netherlands 2011).

[82] For an overview of the conditions needed for the Brussels Effect, and the effects of their absence, see BRADFORD, *supra* note 8, ch. 2.

[83] *Id.* at 26–30.

[84] See generally Alex Engler, *The EU AI Act Will Have Global Impact, but a Limited Brussels Effect*, BROOKINGS (Aug. 6, 2022), https://www.brookings.edu/research/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/.

[85] National governments and the EU institutions themselves are eager to adopt AI technologies: Colin van Noordt & Gianluca Misuraca, *Artificial intelligence for the public sector: results of landscaping the use of AI in government across the European Union*, 39 GOV'T. INFO. Q. 101714, 9–11 (2022).

[86] BRADFORD, *supra* note 8, at 30–37.

[87] In fact, part of the appeal of AI technologies resides not on their current capabilities, but on their *promises* of future results: Hartmut Hirsch-Kreinsen, *Artificial Intelligence: A "Promising Technology,"* AI & SOC'Y. early access, 9–10 (2023). This speculative character often lends itself to overstated claims, both by AI proponents and its critics. For some examples, see generally Franz Seifert & Camilo Fautz, *Hype After Hype: From Bio to Nano to AI*, 15 NANOETHICS 143 (2021); Inioluwa Deborah Raji et al., *The Fallacy of AI Functionality*, 2022 ACM Conference on Fairness, Accountability, and Transparency 959 (ACM Jun. 2022).

[88] Nemitz, *supra* note 2, at 8–10.

[89] See generally AI HLEG, Policy and Investment Recommendations for Trustworthy AI (Jun. 2019).

[90] Such as the *European Centre for Algorithmic Transparency*, EUROPEAN COMMISSION, https://algorithmic-transparency.ec.europa.eu/index_en (last visited Mar. 27, 2023).

[91] Mazzini & Scalzo, *supra* note 20, at 3–4.

[92] Exceptions include the United States and China. Indeed, the US National Institute of Standards and Technology and the Cybersecurity Administration of China are relevant soft-law sources in the field of AI regulation. See generally NIST, *AI Risk Management Framework: AI RMF (1.0)*, No. NIST AI 100-1 (2023); Helen Toner et al., *Translation: Internet Information Service Algorithmic Recommendation Management Provisions*, DIGICHINA (Oct. 1, 2022), https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/.

[93] See, e.g., Cecil Abungu, *Algorithmic Decision-Making and Discrimination in Developing Countries*, 13 CASE W. RES. J.L. TECH. & INTERNET 39, 64 (2022).

A Brussels Effect for the AI Act also requires *stringency*.[94] If the EU standards are more demanding than those of other jurisdictions, compliance with the former is likely enough for the latter, too. Here the AI Act stands on less solid ground. Regarding systems that are neither prohibited nor classified as high-risk, the AI Act does not establish any new rules, except for the transparency requirements that apply to certain applications under Article 52 AI Act. But some jurisdictions have proposed stricter rules for particular applications, such as online recommender systems.[95] Others have proposed additional rules for non-high-risk AI, which often rely on mechanisms beyond the technical requirements imposed by the AI Act.[96] Conformity with the AI Act might therefore be insufficient to ensure a low-risk AI system complies with the laws of any potential jurisdiction.

Contrastingly, the comprehensive approach adopted in the AI Act for high-risk AI systems will be stringent in the matters it covers.[97] But, as discussed in Part A.II *supra*, some of the public interest concerns driving AI are not covered by a product safety framework, as is the case of important dimensions of fundamental rights. Any third-country legislation that directly touches upon issues not covered by the AI Act will thus create requirements that go beyond the EU requirements. The AI Act can only be said to be stringent regarding its list of prohibited AI systems and, for high-risk AI systems, on the issues covered by the product safety framework.

An additional requirement for a Brussels Effect is that regulation must be directed at an *inelastic target*: a product or producer that must be tied to a regulatory regime regardless of its characteristics.[98] In the case of the AI Act, it is possible to identify two different forms of elasticity. The first one concerns its scope: if providers could simply provide their AI systems from outside the EU, they would have little incentive to comply with a more stringent framework, let alone extend it worldwide. But the AI Act curtails this possibility through a territorial extension mechanism,[99] which makes its provisions applicable to any AI system that has its outputs used within the EU, even if its providers—or even users—are based in a third country.[100] In theory, nothing prevents a provider from leaving the EU market altogether or not entering it in the first place, but the market size outlined *supra* might prove too tempting for most large-scale providers.[101] And, once the decision to enter the EU single market is made, providers have minimal room for maneuver to avoid the Act's scope.[102] Therefore, the providers of AI systems used within the EU, or towards persons based in the EU, cannot dodge the AI Act.

A second form of elasticity might happen *within* the AI Act's framework. Once a system is subject to the Act, it is assigned to one of the three regulatory frameworks presented in Part II.A *supra*, and it might also be subject to additional rules targeted at specific classes of systems.[103] To reduce

[94] BRADFORD, *supra* note 8, at 37–48.
[95] See generally Toner et al., *supra* note 92.
[96] Such as the individual rights proposed in the Brazilian AI bill: see generally Sakiotis et al., *supra* note 72.
[97] This hypothesis is grounded on the level of detail in the AI Act and its accompanying standards and the global diffusion of the EU approach to product safety: Siegmann & Anderljung, *supra* note 21, at 78–80.
[98] For example, consumer markets are quite inelastic because a producer must meet a jurisdiction's requirements before serving that market, whereas stock markets are more elastic because of the possibilities afforded by international capital flows: BRADFORD, *supra* note 8, at 48–53.
[99] See generally Joanne Scott, *Extraterritoriality and Territorial Extension in EU Law*, 62 AM. J. COMP. L. 87 (2014).
[100] Article 2(1)(b) AI Act.
[101] For example, the CEO of OpenAI made public remarks in May 2023 to the effect that the AI Act might prompt the company to withdraw its tools, such as ChatGPT, from the EU markets. This threat, however, was publicly abandoned in the same week it was made: Shiona McCallum & Andrew Vance, *ChatGPT-Maker U-Turns on Threat to Leave EU over AI Law*, BBC NEWS (May 25, 2023), https://www.bbc.com/news/technology-65708114.
[102] Siegmann & Anderljung, *supra* note 21, at 39.
[103] Such as the transparency requirements from Article 52 AI Act.

their obligations, providers might argue that their system should be classified in a category that is less stringently regulated.[104] This risk is mitigated to some extent by the Act's top-down approach to risk, as providers can only avoid classification if they show that their system is not designed for one or more of the applications flagged as high-risk by the legislator.[105] As a result, each of the AI Act's regulatory subsystems is inelastic to a certain degree.

Finally, the Brussels Effect also requires *non-divisibility* of the regulated object.[106] If providers can create separate AI systems for the EU market, they do not need to comply with EU standards in other jurisdictions. This non-divisibility is entirely absent from the regulation of prohibited AI systems, as providers can simply continue commercializing these systems in jurisdictions that allow so.[107] Some lawful applications, such as AI systems made for the public sector and other tailor-made applications, are also amenable to segmentation, as these products are already highly differentiated for their customers.[108] AI markets such as those are, therefore, unlikely to see a substantial Brussels Effect.

Still, the current approaches to AI promote non-divisibility in other applications. Most current advances in AI technologies rely on machine learning systems, which require vast amounts of data and extensive computing capabilities.[109] Only a few economic actors have the resources necessary to create such systems.[110] As a result, most AI providers build their AI systems compositionally, starting their work from components—or even fully-trained models—offered by these large-scale providers,[111] who effectively become suppliers of digital infrastructure.

The compositional construction of AI technologies reinforces the AI Act's likelihood of avoiding divisibility. To the extent that AI technologies rely on centralized infrastructures, including general-purpose AI systems,[112] they preclude smaller providers from spinning off EU-specific versions of their products, and even large providers might find that the costs of maintaining an EU-specific version of their technical infrastructure might prove to be excessive. In those cases, market segmentation might be a financially unsound move, because creating EU-specific products is more expensive than global compliance with EU law requirements. Similarly, this reliance on components and general-purpose AI tools promotes non-divisibility within the EU market, as low-

[104] As an example from beyond the AI Act, EU data protection law imposes stringent rules for automated decision-making systems: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 22. In the judicial and administrative disputes concerning this provision, one of the key issues tends to be whether a computer system meets the standards for automated decision-making or whether there is enough human involvement in the decision to make the rules of Article 22 GDPR inapplicable: Katerina Demetzou et al., *The Thin Red Line: Refocusing Data Protection Law on ADM, a Global Perspective with Lessons from Case-Law*, 49 COMPUT. L. & SEC. REV. 105806, 4–7 (Jan. 2023).

[105] The Parliament's political compromise introduces a new form of elasticity: the providers of systems created for applications listed in Annex III AI Act can avoid the high-risk label if they show their system does not impose substantial risks to health, safety, or fundamental rights: Benifei & Tudorache, *supra* note 18, art. 6(2a).

[106] Siegmann & Anderljung, *supra* note 21, at 54–62.

[107] See generally Salvatore Orlando, Regole di imissione sul mercato e «pratiche di intelligenza artificiale» vietate nella proposta di Artificial Intelligence Act, 2022 PERSONA E MERCATO 346 (2022).

[108] Siegmann & Anderljung, *supra* note 21, at 48.

[109] See generally Matthias Gallé, Foundation Models in AI: What Impact for Policies and Law? (May 2022).

[110] Siegmann & Anderljung, *supra* note 21, at 30.

[111] See generally Jennifer Cobbe & Jatinder Singh, Artificial Intelligence as a Service: Legal Responsibilities, Liabilities, and Policy Challenges, 42 COMPUT. L. & SEC. REV. (2021).

[112] See generally Philipp Hacker et al., *Regulating ChatGPT and Other Large Generative AI Models*, No. arXiv:2302.02337 (arXiv Dec. 2023).

risk AI systems built with general-purpose tools will comply with some of the tool's technical requirements.[113]

Based on the brief overview presented *supra*, we agree with studies that suggest a limited Brussels Effect for the AI Act.[114] Market factors alone are insufficient to globalize the EU standards on prohibited AI systems or, indeed, on AI systems falling outside the category of high-risk AI. Even within the latter category, the spread of EU standards depends on the possibility of product differentiation and the extent to which product safety framework addresses relevant regulatory concerns. Yet, the technical complexity involved in governing AI increases the difficulty of identifying—at least *ex ante*—situations in which other standards are more stringent than the EU approach. The EU standard for high-risk AI is, therefore, likely to shape the governance of these applications around the world. But, as we shall see *infra*, this success in spreading the AI Act framework comes at a price.

B.II The Risk of a Brussels Side Effect

To put it shortly, a Brussels Effect for the AI Act will produce a noticeable side effect: a reduced level of protection of these values that cannot be framed as product safety requirements. The global diffusion of AI safety standards based on the AI Act offers, therefore, insufficient protection for values such as fundamental rights, democracy, and the rule of law. Even worse: standards based on the AI Act can introduce new risks to these values by imposing norms guided by a restrictive view of them. If these shortcomings of the AI Act are not addressed during its legislative process, the Brussels Effect can lead to a global weakening of values that are dear to the EU legal order.

We postulate through mechanisms through which the global diffusion of standards based on the AI Act might weaken the protection of fundamental rights, the rule of law, and other high-level democratic values. First, the aforementioned side effect can be produced *de facto* through compliance with the AI Act's technical requirements. Most technical requirements, such as those formulated through technical standards, supply an extensive list of factors that must be observed in their implementation.[115] Given the EU's reputation for stringent regulation, providers, users, and the general population are likely to believe that conformity with a standard, or certification scheme, that complies with the AI Act is enough to protect fundamental rights and other values.[116] Yet, Part A.II *supra* suggests that such an assumption can break down if the values are formulated in general terms or are not amenable to translation into software rules. If the providers of AI systems are nonetheless expected to comply with the product safety requirements imposed by the AI Act, those fuzzier regulatory goals that escape the product safety framework are likely to be deprioritized in the software design process. Consequently, risks to values not covered by the AI Act might only be detected once they have materialized into harm to individuals and social groups.

Adverse consequences may also emerge from the *de jure* form of the Brussels Effect. Such an occurrence, however, is less likely than the *de facto* variant outlined *supra*. Most jurisdictions are not subject to the competence constraints that led the EU to frame the AI Act as a product safety

[113] More speculatively, one should not discard the possibility that some providers of general-purpose AI end up adopting some or all the requirements for high-risk AI to pitch their systems as suitable components for high-risk applications.
[114] See generally Engler, *supra* note 84; Siegmann & Anderljung, *supra* note 21.
[115] On the complexity of technical standardization, see generally JoAnne Yates & Craig Murphy, Engineering Rules: Global Standard Setting since 1880 (Johns Hopkins University Press 2019); Brice Laurent, European Objects: The Troubled Dreams of Harmonization (The MIT Press 2022).
[116] See the diffusion of the CE markings in product safety: Siegmann & Anderljung, *supra* note 21, at 79.

instrument. Accordingly, they have the power to adopt other approaches to regulation or to supplement product safety regulation with rights-based instruments or other regulatory tools.[117] But most forms of AI regulation proposed so far rely extensively on technical knowledge and resources,[118] which can be in short supply for many jurisdictions.

On the one hand, this technical scarcity might prompt some jurisdictions to adopt regulations more in line with their existing capabilities.[119] On the other hand, some jurisdictions might outsource the management of regulatory complexity to the EU.[120] So, legislators worldwide might find themselves replicating the advantages and shortcomings of the AI Act even if they could theoretically do otherwise.

Should the possibility of external side effects from the AI Act be considered in its legislative procedure? A political realist might point out that the EU acts within its powers if it enacts a product safety regulation, and that it has neither the power nor the duty to care about the implications outside the Union's borders. Such a position, however, would be at odds with the EU's constitutional duty to promote European values in its relations with the wider world.[121] And, specifically in the case of the AI Act, it would clash with the stated policy goal of using AI regulation as a vehicle for the global promotion of European values.[122]

The Brussels Side Effect postulated in the title of this paper emerges, therefore, from the peculiar configuration of the AI Act. Given the internal requirements of AI law, the AI Act was shoehorned into a product safety framework. This framework fails to attend to values the EU is constitutionally required to observe, such as respect for democracy, the rule of law, and fundamental rights.[123] It is nonetheless likely to become a global standard, at least for high-risk applications, to the extent that the market on AI technologies satisfies the conditions for a Brussels Effect. Under these circumstances, the EU's ambitions of spreading a European approach to AI are derailed by its very success in exporting regulatory standards to the world.

C AI Regulation Between the EU and the Council of Europe

While the EU has pioneered the idea of a comprehensive approach to AI regulation, other jurisdictions and international organizations are also crafting their approaches.[124] As of 2023, one of the most advanced proposals in this regard is the one formulated by the Council of Europe (CoE), an international organization formed by 46 Member States, including all of the EU's Member States. Because of this direct overlap between the EU's territorial scope and the potential parties of a CoE treaty on AI, we now turn our analysis to the CoE's proposal and its interactions with the AI Act.

[117] Some scholars have argued for radically different approaches to AI regulation: see generally AI HLEG, *supra* note 89; Edwards, *supra* note 53; Margot E. Kaminski, *Regulating the Risks of AI* (Sep. 2022). And the current version of the Brazilian AI Bill adopts a mostly rights-based approach: Projeto de Lei n° 2338, Senado Federal (2023).

[118] Except, perhaps, for regulatory approaches based on principles and ethical guidelines, but even those will need to bridge the gap between abstract principles and the technical nuance of real-world uses of AI.

[119] See generally Abungu, *supra* note 93.

[120] BRADFORD, *supra* note 8, at 253.

[121] Article 3(5) TEU.

[122] Commission, *supra* note 1, at 8.

[123] Article 2 TEU.

[124] See generally Mireille Hildebrandt, *Global Competition and Convergence of AI Law*, *in* ELGAR ENCYCLOPEDIA FOR COMPARATIVE LAW (Jan M. Smits et al. eds., Edward Elgar 2023).

Since its foundation in 1949, the CoE has acted to protect human rights in Europe. Its activities are directed at protecting and promoting its three pillars: Human Rights, Democracy, and the Rule of Law.[125] For these purposes, the CoE carries out various activities, notably the elaboration of treaties on topics that affect one or more of these pillars. And it is in this capacity that the CoE enters the domain of AI regulation.

Given the potential impact of AI technologies on human rights, democratic values, and the rule of law, the CoE set up in 2019 an *ad hoc* Committee on Artificial Intelligence. This committee, grounded on the Human Rights pillar of the CoE's competencies,[126] was set up to examine the feasibility and the potential elements of a convention to deal with the new and future threats posed by AI systems.[127] The main result of this work, delivered by the end of 2021, was a feasibility study of a legal framework for the development, design, and application of AI based on CoE's three pillars.[128]

After delivering this feasibility study, the *ad hoc* committee was substituted by a new advisory body: the Committee on Artificial Intelligence (CAI). The new committee is meant to follow up on the previous work and draft an "appropriate legal instrument on the development, design, and application of AI systems based on the CoE's standards on human rights, democracy, and the rule of law, and conducive to innovation, in accordance with the relevant decisions of the Committee of Ministers."[129] The addition of "innovation" as a guiding concern for CAI suggests that the resulting instrument is expected to tackle a problem that also appears in the AI Act:[130] how to foster the adoption of AI technologies while protecting fundamental public interests.[131]

In February 2023, the CAI decided to publish a "Zero draft" of its intended Convention on AI, Human Rights, Democracy, and the Rule of Law.[132] This publication was accompanied by a disclaimer that the draft 'does not reflect the final outcome of negotiations in the Committee'.[133] Still, the published text suggests some convergences and divergences between the CAI's view of how to regulate AI and the EU's approach in the AI Act.

The similarities cover essential aspects of both proposals. Beyond the similarity in the formulation of CAI's goals and those guiding the AI Act, they also adopt similar framings to the object of regulation. The CAI text stipulates that AI regulation is directed at the development, design, and application of AI systems,[134] which must be regulated throughout their entire life cycle.[135] Both

[125] *About the Council of Europe*, COUNCIL OF EUROPE OFFICE IN UKRAINE, https://www.coe.int/en/web/kyiv/the-coe/about-coe (last visited Jun. 8, 2023).
[126] Article 1 Statute of the Council of Europe (1949).
[127] Terms of Reference for the Ad Hoc Committee on Artificial Intelligence (CAHAI). Extract from CM(2019)131-Addfinal. 1 (Council of Europe 2019).
[128] Council of Europe, *Feasibility Study*, No. CAHAI(2020)23 (Dec. 2020).
[129] Terms of Reference for the Committee on Artificial Intelligence (CAI). Extract from CM(2021)131-Addfinal 1 (Council of Europe 2021).
[130] See Part A *supra*.
[131] This language is parallel to the dual objectives of the AI Act discussed in Part A *supra*. Further studies are needed before any claims that the AI Act *caused* this shift.
[132] Council of Europe, Revised Zero Draft [Framework] Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, No. CAI(2023)01 (Jun. 2023).
[133] CAI, 4th Meeting; 1-3 February 2023. List of Decisions, No. CAI(2023)05, 4 (2023).
[134] Article 4(1) of the Zero Draft.
[135] Article 4(2) of the Zero Draft. On the grounding for this decision, see Catelijne Muller, *The Impact of AI on Human Rights, Democracy and the Rule of Law*, *in* TOWARDS REGULATION OF AI SYSTEMS: GLOBAL PERSPECTIVES ON THE DEVELOPMENT OF A LEGAL FRAMEWORK ON ARTIFICIAL INTELLIGENCE SYSTEMS BASED ON THE COUNCIL OF EUROPE'S STANDARDS ON HUMAN RIGHTS, DEMOCRACY AND THE RULE OF LAW 21 (Council of Europe Dec. 2020).

instruments establish substantive requirements for protecting human and fundamental rights,[136] which apply to the uses of AI systems in the public and private sectors.[137] And they both propose horizontal rules for AI that coexist with other legal instruments: the CoE has treaties on data protection[138] and cybercrime,[139] while the AI Act coexists with EU data protection law[140] and recent regulations on the digital single market, such as the Digital Markets Act[141] and the Digital Services Act.[142] Similar needs and concerns have introduced much convergence between the EU and the CAI approach AI regulation.

Yet, the divergences between both approaches might be even more substantial. As we have seen in Part A *supra*, the AI Act adopts a risk-based approach with a clear focus on high-risk AI systems. Contrastingly, the CAI approach combines a risk-based approach with principle-based elements,[143] which allows it to specify a genuinely horizontal method by setting up principles that apply to all AI applications within its scope. This is not to say that the CAI ignores risk judgments entirely, as it includes obligations for a risk management framework.[144] But risk classification in the CAI proposal happens *after* determining the applicable rules,[145] whereas the AI Act approach looks at risk *before* determining the applicable regulatory regime for an AI system.

Another distinction between the AI Act and the Zero Draft comes from the values protected by each approach. While the AI Act claims to pursue various public interests,[146] it only includes rules on the protection of fundamental rights, which are mostly construed by appending "and fundamental rights" to product safety provisions that require providers to address risks to health and safety. The Zero Draft, instead, includes general principles such as equality, non-discrimination,[147] human dignity, privacy, accountability, transparency and oversight, and safe innovation, as well as the need for inclusive democratic processes, the preservation of public health, and the environment.

To support these manifold goals, the CAI supplements the Zero Draft with a draft methodology entitled the Human Rights, Democracy and the Rule of Law Risk and Impact Assessment (HUDERIA). This methodology seeks to supply 'clear, concrete and objective criteria' to identify sensitive contexts in which AI systems are likely to pose 'significant levels of risk to the enjoyment of human rights, the functioning of democracy and the observance of the rule of law.'[148]

[136] In the Zero Draft, see Article 6.
[137] In the Zero Draft, see Article 5.
[138] Modernised convention for the protection of individuals with regard to the processing of personal data (Convention 108+), CETS 181 (2018).
[139] Convention on Cybercrime, CETS 185 (2001).
[140] For a brief overview of the EU data protection framework and its evolution, see generally Eleni Kosta, *A Divided European Data Protection Framework: A Critical Reflection on the Choices of the European Legislator Post-Lisbon*, *in* RESEARCH HANDBOOK ON EU DATA PROTECTION LAW 68 (Eleni Kosta & Ronald Leenes eds., Edward Elgar Publishing 2022).
[141] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (Text with EEA relevance), 2022 O.J. (L 265) 1.
[142] 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) (Text with EEA relevance), 2022 O.J. (L 277) 1.
[143] Article 1(1) of the Zero Draft.
[144] Article 24 of the Zero Draft.
[145] See generally Victoria Hendrickx & Peggy Valcke, *The Council of Europe's Road towards an AI Convention: Taking Stock*, LAW, ETHICS & POLICY OF AI (Jan. 25, 2023), https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/AI-Council-of-Europe-draft-convention.
[146] Recital 1 AI Act.
[147] Including an explicit prohibition of discrimination 'based on a combination of one or more of the [safeguarded] grounds': Article 3 Zero Draft.
[148] Outline of HUDERIA Risk and Impact Assessment Methodology, No. CAI-BU(2022)03 (May 2022).

Additionally, HUDERIA lays down procedural mechanisms to ensure risk and impact assessment, access to remedies, and regular monitoring to be put in place by AI developers, users and intermediaries. This holistic approach to risk assessment stands in clear contrast with the product safety mechanisms discussed in Part A *supra*, so the full vision of the CAI for AI regulation departs more deeply from the AI Act than the divergences we identified in the Zero Draft.

Such divergences, in turn, create a few issues for the AI Act's potential Brussels Effect. If the CAI approach turns out to be more stringent than the EU's, as is likely to be the case in matters of democracy and the rule of law that fall outside the scope of the AI Act, the EU instrument loses some of its appeal as a global standard.[149] In contexts that involve some overlap between the AI Act and the CAI instruments, there is also the risk of inconsistencies between the regulatory approaches. These inconsistencies may follow from the differences between the product safety and principle-based approaches to regulation,[150] or from differences in balancing market imperatives and human rights (and, in the case of the CAI approach, democratic values and the rule of law). Either way, the resolution of these inconsistencies will pose problems to jurisdictions that must apply, at the same time, AI Act-style requirements and CAI-style requirements.[151]

How to resolve these potential clashes between the instruments? Because the AI Act is constrained by institutional limits to the EU competencies,[152] it cannot be altered to match the full scope of the CAI approach. So, any convergence between these two instruments would come in one of two ways: either the AI Act's scope is reduced, or the CAI provisions become more similar to the AI Act.

Under the former approach, the AI Act would be stripped of its fundamental rights requirements, which would be covered by the CAI approach to human rights. Such a reframing would cast the AI Act as a pure product safety instrument, removing the need for the compromises made to extend the framework for protecting fundamental rights. But it would require the EU to cede its role in defining fundamental rights rules in AI regulation. While all 27 EU Member States, and the EU itself, participate in the CAI, the negotiations for an international law instrument involve all 46 CoE Member States, as well as some observer States such as Canada, Israel, Japan, Mexico, and the United States.[153] Any rules on fundamental rights produced in this context would be heavily influenced by EU perspectives, and they would also entail some compromise between EU values and interests and those of non-EU parties involved in the negotiation.[154]

The EU has decided, instead, to solve any conflicts between the AI Act and the CAI approach by influencing the CoE towards the former. In November 2022, the Council of the EU authorized the Commission to start negotiations on behalf of the EU,[155] with a view to ensuring consistency between both approaches.[156] The specific positions the Commission is expected to pursue are

[149] On the importance of stringency for the Brussels Effect, see Part B.I *supra*.
[150] See Almada & Petit, *supra* note 40, at 13–18.
[151] The EU Member States would be in this position, as they are also parties to the CoE and involved in the CAI negotiation procedure. But similar issues would face any jurisdiction that is pushed towards the AI Act, even if partially, through the Brussels Effect.
[152] See Part A *supra*.
[153] *The Council Of Europe's Relations with Observer States*, COUNCIL OF EUROPE, https://www.coe.int/en/web/der/observer-states (last visited Jun. 9, 2023).
[154] On the diverse perspectives held by nations on matters of AI regulation, see Isaac Ben-Israel et al., Towards Regulation of AI Systems: Global Perspectives on the Development of a Legal Framework on Artificial Intelligence Systems Based on the Council of Europe's Standards on Human Rights, Democracy and the Rule of Law, No. DGI (2020)16 (Dec. 2020).
[155] Council Decision (EU) 2022/2349 of 21 November 2022 authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law, 2022 O.J. (L 311) 1.
[156] *Id.* Recital 7.

detailed in an addendum to the decision, which—at least in its draft version—states that the Union should push the CoE towards a risk-based approach[157] that is fully compatible with the AI Act[158] and recognizes an important role for technical standards and certification mechanisms.[159] In short, the Commission's position in the negotiations should be that of shaping the CoE convention into an approach that bears the core elements of the AI Act.

This direct exercise of influence in the negotiations cannot be mistaken for a Brussels Effect, as it requires the EU[160] to act in a multilateral forum. Yet, this multilateral action is intricately connected to the EU's unilateral influence in regulation. On the one hand, the potential replication of AI Act provisions into the CoE convention removes a potential competitor to the AI Act in the global sphere. On the other hand, any Brussels Effect from the AI Act can strengthen the EU negotiating position if it comes before the convention's provisions are fully defined.[161] So, the EU's position in the CoE negotiations is coherent with its ambitions to shape the regulation of AI technologies globally. The side-effects of regulating AI through a product safety approach might therefore harm the protection of fundamental rights, democracy, and the rule of law, both in the EU and worldwide.

D Conclusion

The arguments *supra* have implications for the theoretical debates on the Brussels Effect and the regulatory debates on AI governance. Our contribution to the scholarship on the Brussels Effect is narrow. While we believe the Side Effect may appear in other areas—particularly in different branches of EU digital regulation—we make no direct attempt to establish its existence elsewhere. Still, these arguments show some of the difficulties in assessing the stringency criteria for the occurrence of the Brussels Effect.

It has been argued, notably by Bradford herself,[162] that the Brussels Effect provides an alternative to the "race to the bottom" models of regulatory competition. As seen in Part A.II *supra*, the existence of a Brussels Side Effect in AI regulation would produce a situation in which the stringent regulatory standards from the AI Act lead to weaker standards for the protection of fundamental rights. Such a scenario suggests the need for distinguishing between the global diffusion of specific regulatory instruments and the diffusion of regulatory goals and framings, which might not accompany—or even be undermined by—the former under the Brussels Effect.

Regarding the regulation of AI technologies, the side-effect mapped in Part B.II *supra* suggests that the AI Act can be a double-edged sword for the EU. On the one hand, it provides a template that will shape other regulatory efforts by the simple fact of being the first substantive regulation on AI, preserving the EU as a global rule-maker. On the other hand, this very efficiency may prevent the EU from developing the instruments it needs to address the shortcomings of the product safety

[157] Recommendation for a Council Decision authorising the opening of negotiations on behalf of the European Union for a Council of Europe convention on artificial intelligence, human rights, democracy and the rule of law, COM(2022) 414 final (2022), point 11.
[158] COM(2022) 414 final, point 12.
[159] COM(2022) 414 final, point 17.
[160] And its Member States, who are expected to support the Commission's positions considering the duty of sincere cooperation present in Article 4(3) TEU.
[161] In fact, the Commission has sought to actively delay negotiations on the convention to give more time for the AI Act's legislative procedure: See generally Luca Bertuzzi, *EU Commission Postponed AI Treaty Negotiations with Further Delays in Sight*, EURACTIV (May 10, 2022), https://www.euractiv.com/section/digital/news/eu-commission-postponed-ai-treaty-negotiations-with-further-delays-in-sight/.
[162] BRADFORD, *supra* note 8, at 52–53.

framework for the regulation of fundamental rights. The European approach to AI may be undermined by the very instrument meant to establish it.

In May 2023, the Parliament committees responsible for the AI Act reached a political compromise regarding the text.[163] This compromise is expected to be approved by the plenary vote by mid-June, kickstarting an interinstitutional process that might produce a final version of the Act by the end of 2023.[164] This timetable, and the institutional constraints surrounding the EU regulatory powers, leave little hope for radical change in the AI Act. But some of its shortcomings might be addressed if the CoE convention is seen as a complement to AI Act, and not merely an instrument for its international diffusion. Otherwise, success in spreading the AI Act might be little more than a Pyrrhic victory for the European approach to AI and its value-setting ambitions.

Acknowledgements
The authors thank Giovanni Sartor, Madalina Busuioc, Chris Marsden, and Gregory Lewkowicz for their comments on this manuscript. They would also like to thank Deirdre Curtin, Nicolas Petit, and Thomas Streinz for their comments on related work.

Marco Almada's work on this paper was partially funded by a Fundación Carolina doctoral grant.

[163] See generally Benifei & Tudorache, *supra* note 18.
[164] Luca Bertuzzi, *Europe's Rulebook for Artificial Intelligence Takes Shape*, THE PRIVACY ADVISOR (May 23, 2023), https://iapp.org/news/a/europes-rulebook-for-artificial-intelligence-takes-shape/.